Certifications have long served as a way to validate security skills, says W. Hord Tipton of (ISC)². But do they remain relevant? **P20**

**Money on a chip**
The Royal Canadian Mint is hoping to make electronic payments just as easy as handing over cash. **PC1**

**A smarter migration**
CISOs must determine how much protection they're willing to contract out for cloud implementations. **P38**

**Exotic, new connections**
Devices never meant to be computers are fast becoming network enabled. **P46**
THE INDUSTRY STANDARD IN MOBILE FORENSICS

Cellebrite UFED makes investigations into mobile device data easier, faster and forensically sound.

EXTRACT AND ANALYZE DATA SUCH AS:
- Email
- File System Data
- Contacts
- Call Logs
- Text messages
- Images & Videos
- Audio Messages
- Phone Passcodes
- GPS fixes
- Deleted and Hidden Data
- and more...

The Cellebrite UFED supports the widest range of mobile devices from all manufacturers, including GPS devices and Chinese Mobile Phones.

1.888.853.0030
forensicsales@cellebriteusa.com
www.facebook.com/CellebriteUFED
twitter: @CellebriteUSA | www.ufedsystem.com

REGULARS
4 Editorial ID thieves find gold in medical data
8 Threat report Online polls in Canada were slowed by a distributed denial-of-service attack
10 Threat stats The biggest increases in month-over-month zombie activity occurred in India
12 Update The Canadian government axed a watchdog responsible for keeping tabs on its spy agency
13 Debate Identifying the culprits behind Kootrace will diminish the gang’s activity
14 Two minutes on ... New election, same risks
15 Skills in demand Software developers are needed to migrate systems to mobile and cloud platforms
16 From the CSO’s desk Bridging corporate and personal, by Michael Scovetta, director at a media company
17 Opinion Can’t we just ignore PCI DSS?, by Mark Kedgley, New Net Technologies
18 Two minutes on ... News, events, same risks
19 Skills in demand Software developers are needed to migrate systems to mobile and cloud platforms
20 Seal of approval Certifications have long validated security skills, says W. Hord Tipton of (ISC)2. But do they remain relevant?
26 In session A selection of some of the schools offering information assurance programs recognized by the NSA and DHS.
31 Assurance on the shore A New Jersey school system found a way to serve increasing broadband needs.
36 A matter of degree The IT field is moving so fast that graduates might be at a disadvantage.
38 A smarter migration CISOs must determine how much cloud security they’re willing to contract out.
40 SC Roundtable: Health hazard IT security pros discuss how risk management can protect patients
46 Exotic, new connections Devices never meant to be computers are fast becoming network enabled.

PRODUCT REVIEWS
49 Product section Students at Norwich University, a Center of Academic Excellence, produced this month’s Group Test for digital forensic tools.
50 Group Test: Digital forensic tools Today’s offerings are characterized by their wide variety of functions, so determining what you need accomplished is key to making the right choice. Too, the integrity and accuracy of recovered media are reliant on the extracting software.

Cover photo by Jay Carlson
Editorial

ID thieves find gold in medical data

Is health care a last frontier for today’s cyber criminals?

According to Paul Contino, corporate chief technology officer at New York City Health and Hospitals Corporation (HHC), it could be – but not for long.

He and other security professionals at a recent SC Magazine Health Care Security Roundtable (see page 40) agreed that because C-level executives in the space continue to sometimes give security needs scant attention, exposures abound. Incidents like the Utah Department of Health breach, which saw about 780,000 individuals’ medical records recently stolen from a server, illustrate what’s to come.

This prediction relies not only on the insecurities rife in health care institutions’ technological infrastructures. Electronic medical records (EMRs) will soon be the norm given the financial support provided by the federal government for taking this route via the Health Information Technology for Economic and Clinical Health (HITECH) Act.

And, what a target EMRs are becoming. According to Contino, medical identity theft is a burgeoning threat likely to grow to huge proportions. In fact, it’s becoming one of the fastest growing crimes in the country, with sophisticated and organized hacking groups stealing patient identities to illegally obtain medical services, prescription drugs, as well as the bank accounts or credit card dollars associated with them. Further, because sharing EMRs among business partners is now the norm, the target only grows larger.

“We’re starting to go outside our four walls, and it’s starting to become a big cloud,” said Contino. “We’re trying to put security around something that at times is a little amorphous.”

Try they must, though. And critical to this is regular risk assessments. “We tend to think we’re ok and oftentimes we’re not,” he said. “Risk assessments need to be there for us to justify to our executives that there is an issue. The sophistication of hacker attempts is getting to the point where it’s incredibly scary.”

Scary, indeed, and those various information and privacy releases we as patients all sign won’t protect health care entities from fines and civil lawsuits any of us might opt to file in the event of our data being breached. As federal auditors continue hitting the pavement in earnest this year to enforce data privacy regulations and the protection of our identities, security and privacy problems in the health care space must be given the attention they deserve.

Ilenna Armstrong is VP, editorial director of SC Magazine.

Privacy problems in health care must be given the attention they deserve.”

“WGU respected the knowledge and experience I already had, making it possible for me to accelerate my program. The curriculum is rigorous and relevant.”
Rich Baich, principal, security & privacy, Deloitte and Touche
Greg Ball, global information protection and security lead partner, KPMG
Christopher Burgess, chief security officer and president, public sector, Alpaca
Jaime Chanana, managing director, CSO Board Consulting
Rufus Connell, research director - information technology, Frost & Sullivan
Dave Cuillienne, chief information security officer, eBay
Mary Ann Davidson, chief security officer, Oracle
Dennis Devlin, assistant vice president of information security and compliance services, George Washington University
Gerhard Eschelbeck, chief technology officer and senior vice president, Symantec
Gene Fredriksen, senior director, corporate information security officer, Tyco International
Maurice Hampton, technical account manager, Qualys
Paul Kurtz, partner and chief operating officer, Good Harbor Consulting
Kris Lowejoy, vice president of IT risk, office of the CIO, IBM
Tim Mathew, director, information protection, KPMG
Stephen Northcutt, president, SANS Technology Institute
Randy Sanovic, former general director, information security, General Motors
Howard Schmidt, cybersecurity coordinator, White House, former president and chief executive officer, Information Security Forum
Ariel Silverstone, former chief information security officer, Expedia
Justin Somain, chief information security officer, Yahoo
Craig Spiezio, chairman, Online Trust Alliance; former director, online safety technologies, Microsoft
W. Horst Tipton, executive director, (ISC)²; former CIO, U.S. Department of the Interior
Amit Yoran, chief executive officer, NetWitness; former director, U.S. Department of Homeland Security’s National Cyber Security Division
* author

WHAT IS SCWC 24/7?
SC Magazine has created a free virtual environment that is open year-round. Each month we host an event focused on a subject that you as an IT security professional face on a regular basis.

THIS MONTH
SC WORLD CONGRESS Symposium
April 24
Cyber espionage
Those engaging in digital spying to steal various classified and/or proprietary documents from U.S. agencies and other organizations are riding high. Foreign adversaries are increasingly launching assaults to steal sensitive economic secrets. The theft of this critical information shows that attackers are enlisting whatever weaknesses in systems they can to steal data, often going unnoticed for months or longer. Experts will share background on the types of systems they can to steal data, often going unnoticed for months or longer. Experts will share background on the types of attacks to watch out for and what to do to thwart them.

ON DEMAND
Data security
Many leading CSOs at various conferences this year touted the need for organizations to have their security controls follow and protect their most important data assets, rather than focusing on the network. So, just how is this best achieved and what plans, policies and technologies can help?

Mobile security
To safeguard handheld devices used by business executives is a constant trial – one that rarely is satisfactorily remedied. But companies must find a way to manage and protect these endpoints.

FOR MORE INFO
For information on SCWC 24/7 events, please contact Natasha Mulla at natasha.mulla@haymarketmedia.com. For sponsorship opportunities, contact Mike Alessie at mike.alessie@haymarketmedia.com.

WHO’S WHO AT SC MAGAZINE
Pakistan top producer of zombie IP addresses

During the past month, the EMEA region (Europe, the Middle East and Africa) was the leading source of all zombie IP addresses. Of the countries making up the EMEA, Pakistan was the top-producing country. For the other regions, the top producers were Brazil in South America, the United States in North America and India in the Asia-Pacific region. (Source: Symantec)
**ThreatStats**

The largest increases in month-over-month zombie activity occurred in India.

### Malware Vertical encounter rate

- **156% Food & beverage**
- **147% Education**
- **113% IT & telecom**
- **106% Retail & wholesale**
- **100% Health care**
- **75% Finance**
- **69% Government**

The biggest increases in month-over-month zombie activity occurred in India, Russia, Vietnam and Morocco, while the largest decreases occurred in Brazil and other Asian nations.

### Spam rate Compared to global email

- **Israel 10.30%**
- **United States 8.16%**
- **Indonesia 6.31%**
- **Japan 4.92%**
- **Taiwan 2.38%**

Spam rate indicates the accumulated emails tagged as unsolicited.

### Top attacks used by U.S. hackers

1. **Downloader trojan**
2. **Butterfly bot**
3. **ZeroAccess trojan**
4. **Gbot trojan**
5. **Chinese Infostealer trojan**

### Top attacks used by foreign hackers

1. **Chinese Infostealer trojan**
2. **ZeuS trojan**
3. **ZeroAccess trojan**
4. **TDSS downloader trojan**
5. **Alureon trojan**

There were 1,994,533 attacks in the United States last month, primarily originating from New York, Rockville, Md., Minneapolis, Kingston, R.I., and Garden City, N.Y. There were 2,490,208 foreign attacks last month, primarily originating from Madrid, Buenos Aires, Argentina, Bucharest, Romania; Santiago, Chile; and Caracas, Venezuela.

---

### DataBank

**Spam**  
The world’s worst spam-support ISPs

<table>
<thead>
<tr>
<th>Position</th>
<th>ISP</th>
<th>Number of current known spam issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>hostroc.net</td>
<td>34</td>
</tr>
<tr>
<td>2</td>
<td>chinanet-cj</td>
<td>65</td>
</tr>
<tr>
<td>3</td>
<td>telefonica.com.ar</td>
<td>52</td>
</tr>
<tr>
<td>4</td>
<td>ovh.net</td>
<td>52</td>
</tr>
<tr>
<td>5</td>
<td>chinanet-tj</td>
<td>47</td>
</tr>
<tr>
<td>6</td>
<td>iliad.fr</td>
<td>47</td>
</tr>
<tr>
<td>7</td>
<td>dacom.co.kr</td>
<td>46</td>
</tr>
<tr>
<td>8</td>
<td>unicrn-cn</td>
<td>45</td>
</tr>
<tr>
<td>9</td>
<td>chinanet-gd</td>
<td>45</td>
</tr>
<tr>
<td>10</td>
<td>gvt.net.br</td>
<td>45</td>
</tr>
</tbody>
</table>

The networks listed knowingly provide service to spam gangs and ignore reports from anti-spam systems and internet users.

### Phishing

**A nine percent decrease in March**

February marked a 30 percent fall in worldwide phishing volume, and March followed with another drop of nine percent. Comparing March with last year, the total number of attacks was also relatively low in the early spring and only started picking up again in May. March 2012 marks a nine percent increase from March 2011's total. Source: RSA Anti-Fraud Command Center

### Top breaches in March Data loss

<table>
<thead>
<tr>
<th>Name</th>
<th>Type of breach</th>
<th>Number of records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department of Child Support Services (Boulder, Colo.)</td>
<td>The agency was notified that contractors IBM and Iron Mountain could not locate several storage devices that had been shipped from Colorado to California.</td>
<td>800,000</td>
</tr>
<tr>
<td>Military Singles.com (New York)</td>
<td>Hackers affiliated with LulzSec claimed responsibility for revealing a database of names, usernames, email addresses, IP addresses and passwords.</td>
<td>171,000</td>
</tr>
<tr>
<td>Digital Playgroup (San Francisco, Calif.)</td>
<td>A group of hackers accessed details on customers and administrators of this pornographic website.</td>
<td>72,794</td>
</tr>
</tbody>
</table>

Total number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005:

**545,645,703** (as of April 2012)

Source: Privacy Rights Clearinghouse (from data provided by DataLossDB.org, hosted by the Open Security Foundation)

### Top breaches in March

- **U.S.**
  - **30,000**
  - **25,000**
  - **20,000**
  - **15,000**
  - **10,000**
  - **5,000**
  - **0**

- **24,019**
- **21,019**
- **21,030**
- **29,974**
- **29,974**
- **29,974**
- **29,974**

**December**

**January**

**February**

**March**

**Top regions**

- **United States 65,645**
- **Russia 50,178**
- **China 26,448**
- **Brazil 19,411**
- **India 12,974**

**Spam sources**

- **26,395**
- **13,099**
- **6,637**

**Global distribution**

- **India 19.2%**
- **Russia 8.3%**
- **Vietnam 6.2%**
- **Morocco 3.8%**
- **Pakistan 5.6%**
- **Brazil 15.4%**
- **China 5.5%**
- **Other Asia 18.8%**
- **Other Europe 71%**

Source: RSA Anti-Fraud Command Center

---

**Internet dangers**

**Top threats**

<table>
<thead>
<tr>
<th>Name</th>
<th>Movement</th>
<th>Data first observed</th>
<th>Type</th>
<th>Last week</th>
<th>Weeks on list</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salty.AT</td>
<td>▲</td>
<td>12/05/10</td>
<td>Virus</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Winwebsec</td>
<td>▼</td>
<td>09/22/10</td>
<td>Scareware</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>Finlinski.A</td>
<td>▲</td>
<td>11/21/10</td>
<td>Backdoor</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>VBlinject.UG</td>
<td>▲</td>
<td>09/11/12</td>
<td>MalwarePackage</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>VBlinject.gnIDS</td>
<td>▲</td>
<td>09/24/10</td>
<td>MalwarePackage</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>Redhop.A</td>
<td>▲</td>
<td>09/21/10</td>
<td>Worm</td>
<td>8</td>
<td>20</td>
</tr>
<tr>
<td>Bitrose.AE</td>
<td>▲</td>
<td>09/23/10</td>
<td>Backdoor</td>
<td>14</td>
<td>2</td>
</tr>
<tr>
<td>Siref.B</td>
<td>▲</td>
<td>09/23/10</td>
<td>Downloader</td>
<td>20</td>
<td>2</td>
</tr>
<tr>
<td>Salty.AU</td>
<td>▲</td>
<td>12/06/10</td>
<td>Worm</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Usteal.D</td>
<td>▲</td>
<td>03/23/12</td>
<td>Spyware</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: Radalert Security Labs

**Top 5 attacks used by foreign hackers**

1. **Chinese Infostealer trojan**
2. **ZeuS trojan**
3. **ZeroAccess trojan**
4. **TDSS downloader trojan**
5. **Alureon trojan**

There were 1,994,533 attacks in the United States last month, primarily originating from New York, Rockville, Md., Minneapolis, Kingston, R.I., and Garden City, N.Y. There were 2,490,208 foreign attacks last month, primarily originating from Madrid, Buenos Aires, Argentina, Bucharest, Romania; Santiago, Chile; and Caracas, Venezuela.

---

**Worldwide phishing volume**

March 2012 marks a nine percent decrease in March.

Source: The Spamhaus Project

**Spam rate**

Source: The Spamhaus Project

**Spam rate**

- **50%**
- **60%**
- **70%**
- **80%**
- **90%**
- **100%**

The chart above reflects the encounter rate of web malware across a selection of industry verticals. Rates above 100 percent reflect a higher-than-median rate of encounter and rates below 100 percent reflect a lower-than-median rate.

Source: Cisco ScanSafe

**Spam rate**

Spam rate indicates the accumulated emails tagged as unsolicited.

**Top 5 attacks used by foreign hackers**

1. **Chinese Infostealer trojan**
2. **ZeuS trojan**
3. **ZeroAccess trojan**
4. **TDSS downloader trojan**
5. **Alureon trojan**

There were 1,994,533 attacks in the United States last month, primarily originating from New York, Rockville, Md., Minneapolis, Kingston, R.I., and Garden City, N.Y. There were 2,490,208 foreign attacks last month, primarily originating from Madrid, Buenos Aires, Argentina, Bucharest, Romania; Santiago, Chile; and Caracas, Venezuela.
**Update**

**NEWS BRIEFS**

- In a budget move last month, the Canadian government used a watchdog responsible for keeping tabs on its spy agency.

- Eva Plunkett, the inspector general of the Canadian Security Intelligence Service (CSIS), had been responsible for monitoring the agency’s activities since 2003. Her post has been removed.

- The decision, which the Canadian government said would save taxpayer money each year, will leave the agency monitored by the Security Intelligence Review Committee. Because of its relatively small size, this body’s oversight of CSIS will be more broad in nature than when Plunkett was in charge.

- In 2020, she highlighted dozens of failures by CSIS to adhere to policy, and noted 43 errors in operational reporting. She called for greater diligence, and pointed to yearly increases in policy breaches.

- Two months before the internet could be shut off to hundreds of thousands of machines, the Canadian government made a website available to help the public check for their susceptibility. The Canadian Internet Registry Authority publicly launched a site (http://www.dns-ok.ca/) in mid-April to check for DNSChanger infections. The DNSChanger trojan is a compromised computer, and requests a website used to create a registry of badly operated servers. These servers then misdirected computers to malicious websites. The Estonian criminals behind DNSChanger were arrested in September, and the DNS servers were replaced with legitimate ones so that those still infected would be safe. However, these benign servers will be disabled on July 9, meaning that the 350,000 computers still infected with the malware will be unable to reach the internet.

- In February, the Canadian government asked CIRA (a member of the Canadian Cyber Incident Response Technical Network) to create its own version. Most users were hit by visiting a malicious website. The trojan has the ability to steal data and hijack search traffic.

- Verizon’s annual “Data Breach Investigations Report” found that hacktivists, whose goal is to name and shame organizations with which they morally disagree, caused just two percent of the incidents studied, but were responsible for 58 percent of the stolen information in 2010. That sits as a notable contrast to previous years, when financially motivated criminals were responsible for the bulk of the hijacked data. The study, in its fifth year, analyzed 855 breaches. The report does not cover infections such as lost or stolen laptops.

**THE QUOTE**

Just when we thought it was safe to go back shopping.

—Avi Litan, vice president and distinguished analyst at Gartner, commenting on a breach in March of payment card processor Global Payments, which put at risk personal data of at least 1.5 million Visa and MasterCard customers.

**SC in Canada**

The conference rooms were packed with information security pros intent on learning the most up-to-date strategies to mitigate threats, the expo floor buzzed with attendees checking out the latest vendor solutions, and SC Awards Canada acknowledged some of the people and companies working to advance the field of information protection and safe computing practices. Click on sccongresscanada for more information.

**Me and my job**

Eva Plunkett, the inspector general of the Canadian Security Intelligence Service (CSIS), had been responsible for keeping tabs on its spy agency. She called for more policy, and noted 43 errors in operational reporting. The third SC Congress Canada in Toronto drew more than 600 attendees.

**Skills in demand**

Software developers with knowledge of cloud needed.

**Debate**

Identifying the culprits behind Koobface will diminish the gang’s activity.

**FOR**

Russia has been known to be a haven for hackers for the past decade or more. It has no jurisdiction over the strangers who are believed to have been behind the malware. So what about the Russians? They are the ones who have been behind so many of the attacks, and they are the ones who have been in the public eye for so long.

**AGAINST**

A most daily I come across data that lead to the (probable) identity of the cyber criminals. The reality is that the numbers of people involved are much larger than we thought. They are the ones who have been behind so many of the attacks, and they are the ones who have been in the public eye for so long.

**THE STATS**

**MS12-020 security bulletin from Microsoft said: “we know of no active exploitation in the wild [of RDP].”**

72 hours after RDP vulnerability revealed, proof-of-concept code was discovered on a Chinese website.

**THE SC MAGAZINE POLL**

Is Windows Remote Desktop Protocol (RDP) exposed at your organization?

- 10.42% Yes
- 16.67% Not sure
- 72.92% No

To take our latest weekly poll, visit www.scmagazine.com

**THREAT OF THE MONTH**

Chrome exploit

What is it? Various vulnerabilities and weaknesses in Google Chrome, which were successfully combined into two separate exploits and demonstrated to execute code outside the sandbox.

How does it work? The first exploit by a skilled Chrome researcher, Sergey Glazunov, combined a universal cross-site scripting vulnerability with a weakness in history navigation to execute code. The second, by a researcher using the handle “PinekPie,” combined three separate vulnerabilities related to plug-in loading and corruption of GPU process memory.

Should I be worried? As these exploits successfully combined multiple vulnerabilities to execute code, users should definitely be careful.

How can I prevent it? Any system running a version of Chrome older than version 170.963.79 should be updated to protect against the vulnerabilities. As Chrome automatically updates to the latest version by default, most systems should already be patched.

Source: Carsten Eiram, chief security specialist, Secunia.
New election, same risks

I n November, Americans will head to the polls to cast ballots in a presidential election. However, the technology used in voting machines has changed little since the last contest, and security risks are still an ever-present danger.

One type of voting system that’s commonly deployed is the Direct Recording Electronic (DRE) machine, a touchscreen device that records votes and processes the data through a computer program. Just as with any internet-enabled computing system, there are inherent security risks are still an ever-present danger.

Even though the applications used in DREs offer software security measures, such as cryptographic signing keys and anti-virus software, they can still be hacked, said John Sebes, CTO of the Trust-TheVote Project, a nonprofit technology think tank. “DREs share the basic hardware architecture of most PCs, where carefully crafted inputs can cause modifications to the software as it executes memory,” he said. “Attacks can, in turn, be used to modify the software or data, including votes.”

In the 2010 Election and Administration Voting Survey, conducted by the U.S. Election Assistance Commission (EAC), an independent, bipartisan agency, 18 states reported deploying DREs, which produce a voter-verified paper audit trail (VVPAT). DREs are also available that do not offer a VVPAT. In Georgia, Maryland, Louisiana, South Carolina, and New Jersey, nearly all voting equipment used in 2010 were DREs without VVPATS.

Three major providers – Election Systems and Software, Sequoia Voting Systems, and Hart Intercivic – supply the electronic voting systems in the United States. Each vendor’s technology has gone through the federal and state certification process, as well as passed the Voting System Testing and Certification Program, developed by EAC.

But, while guidelines and procedures on the federal and state level aid in the overall security, there is still potential for insider attacks in the manufacturing process, Sebes said. As well, hardware or vote-counting software could be altered before it gets to election officials. Although voting equipment may have vulnerabilities, perhaps an even bigger concern involves physical security, said Marcus Machtel, vice president of products at Hart Intercivic, a provider of election voting systems.

“There has been a lot more scrutiny in terms of procedures and what jurisdictions are doing to ensure that the chain of custody is maintained for the machines,” he said. – Marcus Colón

91m individuals voted on Election Day in 2010

Source: EAC

JOBS MARKET

Me and my job

Brian Wolfinger

VP of electronic discovery & forensic services, LDiscovery

How do you describe your job to average people?

I thanks to TV shows like CSI and NCIS, most people have some general idea of what it means to collect evidence. I usually explain that we collect and examine evidence from the electronic devices that fill our lives. Sometimes the evidence is for a civil lawsuit. Other times it is for a criminal matter. Many times people don’t think of electronic evidence in terms of non-criminal matters, so I usually offer up the example of the person who leaves “Company A” and then goes to “Company B,” its direct competitor. Company A may use us to see whether their former employee took formulas, customer lists or other proprietary information with them.

What do you think needs more attention?

I think digital forensic practitioners need to be aware of, and become more involved in, the recent actions in some states that require private investigators’ licensure for those who offer digital forensic services. This is a bad fit.

What security threats are overblown?

While not a security threat per se, the effect(s) of cloud computing on our arena (digital forensics and electronic discovery) seems to have some practitioners and attorneys worried. I think that we will need to make changes and learn new techniques as practitioners, but I don’t see cloud computing as presenting the problems that others envision.

What annoys you?

“Black Box” solutions that offer to solve all of a company’s (or vendor’s) e-discovery needs. These “solutions” don’t solve the problems they claim they do. They tend to be selling tools, not technical offerings, and they make it more difficult for vendors who are trying to address a client’s needs honestly.

What would you use a magic IT security wand for?

I’d eliminate spam. I think the electronic world could use the bandwidth.

Briefs

Company news

CloudLock, a Waltham, Mass.-based cloud data security firm, has secured $8.7 million in Series B funding from Ascent Venture Partners and Cedar Fund. The cash injection will be used to expand the company’s engineering divisions, develop new platforms and pump up sales efforts. CloudLock CTO Gil Zimmermann said the funding also will help the company attract talent. Luke Burns, partner with Ascent, is leading the investment and will join CloudLock’s board. www.cloudlock.com

Blue Coat Systems, a Sunnyvale, Calif.-based provider of web security and WAN optimization solutions, has appointed David Murphy president and chief operating officer, reporting directly to CEO Greg Clark. Murphy, who has 25 years of security, infrastructure and networking experience, will lead the sales and marketing organizations and execute the company’s go-to-market and channel strategies. He was formerly SVP at HP and president and general manager of IBM Tivoli. www.bluecoat.com

Avira, a Teltang, Germany-based global supplier of security solutions, has appointed Dan Hubbard as CTO. Hubbard is tasked with developing products and strategies that enable enterprises to better anticipate internet threats and more intelligently protect against them, across all internet-connected devices. Hubbard has more than 20 years of experience in the security space. He was previously CTO at Websense. www.opendns.com

Industrial Defender, a Foxborough, Mass.-based global provider of security, compliance and change management solutions for automation systems, and Good Harbor Consulting, an Arlington, Va.-based provider of global strategic cyber risk management services, have teamed up to assist critical infrastructure operators improve their cyber security posture. Industrial Defender’s solutions monitor, manage and protect critical infrastructure. Richard Clarke, chairman and CEO of Good Harbor, and formerly special adviser on cyber security to President George W. Bush, said the collaboration will enable executives to manage dynamic cyber risks and protect critical systems. www.industrialdfender.com www.goodharbor.net

Stay updated

Follow us on Facebook and Twitter

Update

Skills in demand

With the popularity of mobile and cloud computing, companies are scrambling to develop applications to combine information from disparate systems and display them in single dashboards. This requires software developers with skills in collaboration software, databases and mobile device programming.

What it takes

Three to five years of experience and certification in collaboration software. Mobile developers need one to three years of C, C++ and Java.

Compensation

Collaborative software developer can earn $100k to $135k, while mobile developers can earn $65k to $95k.

Source: Jerry Irvine, CIO, President Solutions, www.presidentsolutions.com

What do you think needs more attention?

I think digital forensic practitioners need to be aware of, and become more involved in, the recent actions in some states that require private investigator licensure for those who offer digital forensic services. This is a bad fit.

What security threats are overblown?

While not a security threat per se, the effect(s) of cloud computing on our arena (digital forensics and electronic discovery) seems to have some practitioners and attorneys worried. I think that we will need to make changes and learn new techniques as practitioners, but I don’t see cloud computing as presenting the problems that others envision.

What annoys you?

“Black Box” solutions that offer to solve all of a company’s (or vendor’s) e-discovery needs. These “solutions” don’t solve the problems they claim they do. They tend to be selling tools, not technical offerings, and they make it more difficult for vendors who are trying to address a client’s needs honestly.

What would you use a magic IT security wand for?

I’d eliminate spam. I think the electronic world could use the bandwidth.

Briefs

Company news

CloudLock, a Waltham, Mass.-based cloud data security firm, has secured $8.7 million in Series B funding from Ascent Venture Partners and Cedar Fund. The cash injection will be used to expand the company’s engineering divisions, develop new platforms and pump up sales efforts. CloudLock CTO Gil Zimmermann said the funding also will help the company attract talent. Luke Burns, partner with Ascent, is leading the investment and will join CloudLock’s board. www.cloudlock.com

Blue Coat Systems, a Sunnyvale, Calif.-based provider of web security and WAN optimization solutions, has appointed David Murphy president and chief operating officer, reporting directly to CEO Greg Clark. Murphy, who has 25 years of security, infrastructure and networking experience, will lead the sales and marketing organizations and execute the company’s go-to-market and channel strategies. He was formerly SVP at HP and president and general manager of IBM Tivoli. www.bluecoat.com

Avira, a Teltang, Germany-based global supplier of security solutions, has appointed Dan Hubbard as CTO. Hubbard is tasked with developing products and strategies that enable enterprises to better anticipate internet threats and more intelligently protect against them, across all internet-connected devices. Hubbard has more than 20 years of experience in the security space. He was previously CTO at Websense. www.opendns.com

Industrial Defender, a Foxborough, Mass.-based global provider of security, compliance and change management solutions for automation systems, and Good Harbor Consulting, an Arlington, Va.-based provider of global strategic cyber risk management services, have teamed up to assist critical infrastructure operators improve their cyber security posture. Industrial Defender’s solutions monitor, manage and protect critical infrastructure. Richard Clarke, chairman and CEO of Good Harbor, and formerly special adviser on cyber security to President George W. Bush, said the collaboration will enable executives to manage dynamic cyber risks and protect critical systems. www.industrialdfender.com www.goodharbor.net

Stay updated

Follow us on Facebook and Twitter

Update

Skills in demand

With the popularity of mobile and cloud computing, companies are scrambling to develop applications to combine information from disparate systems and display them in single dashboards. This requires software developers with skills in collaboration software, databases and mobile device programming.

What it takes

Three to five years of experience and certification in collaboration software. Mobile developers need one to three years of C, C++ and Java.

Compensation

Collaborative software developer can earn $100k to $135k, while mobile developers can earn $65k to $95k.

Source: Jerry Irvine, CIO, President Solutions, www.presidentsolutions.com

What do you think needs more attention?

I think digital forensic practitioners need to be aware of, and become more involved in, the recent actions in some states that require private investigator licensure for those who offer digital forensic services. This is a bad fit.

What security threats are overblown?

While not a security threat per se, the effect(s) of cloud computing on our arena (digital forensics and electronic discovery) seems to have some practitioners and attorneys worried. I think that we will need to make changes and learn new techniques as practitioners, but I don’t see cloud computing as presenting the problems that others envision.

What annoys you?

“Black Box” solutions that offer to solve all of a company’s (or vendor’s) e-discovery needs. These “solutions” don’t solve the problems they claim they do. They tend to be selling tools, not technical offerings, and they make it more difficult for vendors who are trying to address a client’s needs honestly.

What would you use a magic IT security wand for?

I’d eliminate spam. I think the electronic world could use the bandwidth.
Bridging corporate and personal

Michael Scovetta
director of advanced technology at a large media/entertainment company

Over the past decade, technology innovations have vastly increased consumers’ expectations and have migrated into corporate environments where there is increasing pressure to make corporate resources available to users on any device – whether a smartphone, tablet or laptop. This must be done whether a smartphone, tablet to users on any device excites these days. Which is what makes the role of a CSO exciting these days. Access to social media adds Scovetta.

Consider a bring-your-own-device (BYOD) policy – Employees use personal devices to access apps, social media, corporate email, and sometimes even to make telephone calls. Technologies such as virtual desktop and application virtualization can help, but there is plenty of room for innovation in this space. Embrace platform agnosticism – Partially as a consequence of BYOD, the days of designing applications to be available on a single platform are over. Users need to access corporate resources using a myriad of devices, with more arriving every day. This notion of heterogeneity can also improve your security posture because investments in security solutions can be applied more effectively across platforms. Improve authentication – It shouldn’t be a surprise to any reader that password-based authentication is terribly broken. Whether passwords are reused, stored in clear text, or simply weak, it’s obvious that neither end-users nor application providers are very good at using passwords. Fortunately, technologies like client-certificates, SAML, OpenID, and OAuth have been available for some time, and can mitigate much of the risk inherent in password-based authentication. A dress for file sharing – E-mail attachments are still typically limited to 10 or 20 megabytes. When larger files need to be transferred, some users will look to online services. Modern enterprise-grade file-sharing solutions can meet users’ needs and enforce compliance with security policies. We’re living in a world where users are no longer content to wait for corporate solutions to catch up to what they use in their personal life. As security professionals, we are in a unique position to help implement technologies that improve security and the user experience at the same time.

30 seconds on...

Opinion

Availing the need to disclose

T he past two years have marked a breakthrough in incidents of targeted cyber attacks that were made public. However, currently, companies typically disclose breaches for one of two reasons: either they have to because the attackers have leaked their data, or they must comply with some sort of disclosure law. New guidelines from the Securities and Exchange Commission – while not actual regulations - will likely change all that, which is a good thing when you consider that many companies simply are unable to keep up with the evolving exploits. In the past year alone, we’ve seen attacks go to the next level, as large, global organizations and government agencies were attacked for commercial, political or military reasons. Public companies already adhere to strong corporate governance, and have to comply with regulations and address irregularities that are flagged or investigated. Breaches should be treated no differently. Companies and their IT departments will have to institute a strong, layered, verifiable security approach to protect their assets and uphold strong brand reputation. While this increase in process may strike some as increased complexity and just one more regulatory hoop to jump through, in the long run, the disclosure laws will actually help companies secure their brand reputation and let consumers make more informed investment choices.

Today’s cyber attacks are designed to evade reactive security controls. To meet the challenge of protecting your brand and reducing reporting complexity, companies need to combine proactive and reactive security controls to maximize coverage. This does not mean implementing a bunch of sliced products. Not only does that slow response time when a threat occurs, it makes compliance a real headache. Instead, look for a solution that can correlate threat information to maximize attack intelligence, provide an optimal defense and simplify reporting if a security breach occurs.

While cyber criminals will continue to develop intricate and dynamic attacks, the best defense today is through the combination of best practices, sound security rules and state-of-the-art technologies.

Can’t we just ignore PCI DSS?

It’s fair to say that organizations have had ample time to achieve an acceptable level of compliance to the Payment Card Industry Data Security Standard (PCI DSS), but what we often see is pushback from the board level when it asks for clear-cut justification for PCI investment. Oftentimes, the pushback comes from within the IT department, which is seeking to avoid the perceived disruption that implementing PCI will cause. Add to this scenario the anecdotal feedback that while acquiring banks promote the need for PCI, they seldom have the focus and continual drive to monitor the status of compliance, making it all too easy for merchants to carry on just as they are.

Regardless of where the resistance or inertia comes from, the consensus is that adopting PCI DSS is a sensible thing to do from a security perspective. But like so many things in life, the common-sense view is outweighed by the perceived pain of achieving it. With PCI, there is no denying that it is complex and is likely to cause disruption, but the benefits ultimately outweigh the pitfalls. With PCI being such a comprehensive framework, big thinkers argue that the requirements should be leveraged to provide security for company information as a whole and to protect against the ever-growing mainstream issue of identity theft. Losing cardholder data is one thing, but risking your customers’ personal information is potentially far more damaging.

Fifty years ago, the state of Wisconsin introduced legislation requiring seat belts in cars, but few people used them because they were uncomfortable. So it was only in 1984, when the first state (New York) made the wearing of a seatbelt compulsory that the real benefits were realized. O nly then did common sense become standard practice. My own personal information protection needs the same treatment.

Mark Kedgley, chief technical officer, New Net Technologies

Bradley Anstis, VP of technical strategy, M86 Security

“Adopting PCI DSS is a sensible thing to do from a security perspective.”

Nothing like friends

If done right, social media resources can bring your company closer to your customers and your employees closer to each other, without compromising security, says Scovetta.

Opinion

Can’t we just ignore PCI DSS?

It’s fair to say that organizations have had ample time to achieve an acceptable level of compliance to the Payment Card Industry Data Security Standard (PCI DSS), but what we often see is pushback from the board level when it asks for clear-cut justification for PCI investment. Oftentimes, the pushback comes from within the IT department, which is seeking to avoid the perceived disruption that implementing PCI will cause. Add to this scenario the anecdotal feedback that while acquiring banks promote the need for PCI, they seldom have the focus and continual drive to monitor the status of compliance, making it all too easy for merchants to carry on just as they are.

Regardless of where the resistance or inertia comes from, the consensus is that adopting PCI DSS is a sensible thing to do from a security perspective. But like so many things in life, the common-sense view is outweighed by the perceived pain of achieving it. With PCI, there is no denying that it is complex and is likely to cause disruption, but the benefits ultimately outweigh the pitfalls. With PCI being such a comprehensive framework, big thinkers argue that the requirements should be leveraged to provide security for company information as a whole and to protect against the ever-growing mainstream issue of identity theft. Losing cardholder data is one thing, but risking your customers’ personal information is potentially far more damaging.

Fifty years ago, the state of Wisconsin introduced legislation requiring seat belts in cars, but few people used them because they were uncomfortable. So it was only in 1984, when the first state (New York) made the wearing of a seatbelt compulsory that the real benefits were realized. Only then did common sense become standard practice. My own personal information protection needs the same treatment.
Digital currency

The Royal Canadian Mint is hoping to make electronic payments just as easy as handing over cash. Danny Bradbury investigates.

MintChip puts Canadian currency on a chip

M oney electronically is via the Interac the current de facto method for sending say. Other than PayPal, or costly and users will carry ones and zeros. It's like carrying actual money in one's pocket, but instead of paper and metal, digital currency is stored on a chip. The currency is then sold to brokers, which then trade it with consumers and businesses. Users who purchase MintaChip valuations have them loaded onto a chip, which is then used to transfer payments to another holder's chip without the transaction being paid uses this key to verify the message. When the two chips agree that the transaction is genuine and unique, the MintaChip values are debited and credited accordingly. The currency is then sold to brokers, which then trade it with consumers and businesses. Users who purchase MintaChip valuations have them loaded onto a chip, which is then used to transfer payments to another holder's chip without the transaction being paid uses this key to verify the message. When the two chips agree that the transaction is genuine and unique, the MintaChip values are debited and credited accordingly. The currency is then sold to brokers, which then trade it with consumers and businesses. Users who purchase MintaChip valuations have them loaded onto a chip, which is then used to transfer payments to another holder's chip without the transaction being paid uses this key to verify the message. When the two chips agree that the transaction is genuine and unique, the MintaChip values are debited and credited accordingly. The currency is then sold to brokers, which then trade it with consumers and businesses. Users who purchase MintaChip valuations have them loaded onto a chip, which is then used to transfer payments to another holder's chip without the transaction being paid uses this key to verify the message. When the two chips agree that the transaction is genuine and unique, the MintaChip values are debited and credited accordingly. The currency is then sold to brokers, which then trade it with consumers and businesses. Users who purchase MintaChip valuations have them loaded onto a chip, which is then used to transfer payments to another holder's chip without the transaction being paid uses this key to verify the message. When the two chips agree that the transaction is genuine and unique, the MintaChip values are debited and credited accordingly. The currency is then sold to brokers, which then trade it with consumers and businesses. Users who purchase MintaChip valuations have them loaded onto a chip, which is then used to transfer payments to another holder's chip without the transaction being paid uses this key to verify the message. When the two chips agree that the transaction is genuine and unique, the MintaChip values are debited and credited accordingly.
WHAT’S THE SECRET TO UNLOCKING A REWARDING CAREER IN INFORMATION SECURITY?
THE PASSWORD IS NSU.

With its distinguished faculty and cutting-edge curriculum, Nova Southeastern University’s Graduate School of Computer and Information Sciences prepares students for leadership roles in information security.

In this era of rapid technological growth, each day brings demands for increased proficiencies of professionals in the information security field.

Located on NSU’s main campus in Fort Lauderdale, Florida, GSCIS has been offering graduate degree programs for over three decades. Students may enroll in traditional evening on-campus, online classes, or combination of both – and complete the M.S. degree in 12 months.

NSU is designated a National Center of Academic Excellence in Information Assurance Education by the U.S. National Security Agency and the Department of Homeland Security. GSCIS’s curriculum in information security meets the NSA Committee on National Security standards 4011, 4012, and 4013.

GSCIS offers Master of Science degrees in a variety of IT fields. Whether you are earning your degree to accelerate your career or prepare for the next technological leap, a degree from NSU will give you the tools you’ll need to remain on the cutting edge.
SAFETY APPROVAL

Certifications have long validated security skills, says W. Hord Tipton of (ISC)². But do they remain relevant? Dan Kaplan finds out.

As its executive director, W. Hord Tipton may run the show at nonprofit (ISC)², which manages the security industry’s flagship certification – the CISSP – but he knows no credential can serve as a silver bullet.

“I once had a CIO at a major [federal government] department ask me how many CISSPs does he need to have to guarantee perfect security,” recalls Tipton, 68, the former CIO of the U.S. Department of Interior. “The answer, of course, is, ‘It’s not possible.’ Even if you have the perfect person in place, and they write you the perfect policy and configure your systems perfectly, but you don’t have compliance with those policies, there isn’t a single thing your security person can do.”

Human error remains the Achilles’ heel of most security operations. An organization can have all of its ducks in a row, but if an employee decides to click on an email attachment claiming to be a work-related document, but which actually turns out to be a trojan for which there is no detection, the most knowledgeable security pro in the world may not be able to save its network from compromise.

Still, education is a necessity, Tipton insists. And while the computer science curricula offered by colleges and universities continues to expand, certifications remain the defining way for security pros to learn the trade (through training for the exam) and for potential employers to assess their abilities. This is particularly important in a market where the cyber security workforce is in far greater demand than there is supply, a disproportion that is accentuated as data protection becomes more critical in light of emerging technologies, such as cloud, and an increasing number of devices becoming network-connected.

The Certified Information Systems Security Professional (CISSP) credential, which received the coveted American National Standards Institute (ANSI) accreditation in 2004, covers a total of 10 domains spanning the core principles required of the information assurance professional. By holding this certification, available once individuals have achieved five years of full-time security work experience, they can demonstrate they have a broad-based understanding of the discipline and are willing to become – and stay – qualified.

“College graduates are not coming out with the [adequate] skills and knowledge,” Tipton says. “I know one of the selling features of the CISSP is it not only validates they have some knowledge of security today, it will keep them tied to the changing nature of that.” (Holders of the credential must undergo 120 continuing professional education (CPE) credits every three years – or they lose it.)

But Tipton admits perplexity sometimes reigns in an industry where there are scores of security certifications, being offered by vendor-agnostic entities like Florida-based (ISC)², as well as security solutions providers, such as Cisco.

“We are working with other organizations to try to be explanatory and be simpler in what our credentials mean,” he says. “What is the value from certifications? It’s a confusing world where you’ve got at least 250 acronyms out there.”

“College graduates are not coming out with the [adequate] skills and knowledge,” Tipton says. “I know one of the selling features of the CISSP is it not only validates they have some knowledge of security today, it will keep them tied to the changing nature of that.” (Holders of the credential must undergo 120 continuing professional education (CPE) credits every three years – or they lose it.)

But Tipton admits perplexity sometimes reigns in an industry where there are scores of security certifications, being offered by vendor-agnostic entities like Florida-based (ISC)², as well as security solutions providers, such as Cisco.

“We are working with other organizations to try to be explanatory and be simpler in what our credentials mean,” he says. “What is the value from certifications? It’s a confusing world where you’ve got at least 250 acronyms out there.”

Rick Bauer, director of research at CompTIA, a Chicago area-based IT trade association, says his organization is bringing providers together so a “roadmap” can be developed that matches certifications to job descriptions.

“I think certifications may have suffered from their friends more than folks...
who don’t believe in them,” says Bauer
of the plethora of acronyms that security
practitioners display beside their names
on business cards, often mockingly
referred to as an alphabet soup.
Bauer helped lead the formation of
the Cyber Security Credentials Collabora-
tive (C3), which consists of vendor-
nuetral certification bodies specializing
in IT security and privacy: CompTIA,
EC Council, GIAC, ISACA and (ISC)².
The stated purpose is to offer a forum
for collaboration that “will result in the
advancement of IT careers, a more pre-
pared workforce, greater insight into how
these certifications are developed and
how they meet the IT needs for organiza-
tions, including governments, private
enterprises, educational institutions and
the public at large.”
Bauer says certifications have suffered
because there are so many of them. As a
result, security pros and hiring managers
often are unsure of their value, which
results in workers not obtaining the cor-
rect cert or organizations being unable to
match a candidate with the right position.
“These are our customers who don’t
understand it,” he says. “We can’t com-
municate the value proposition of certifi-
cations, and it’s really important for us to
help to inform the workplace.”
Arguably there is no place feeling the
pressure more when it comes to security
hiring than the federal government.
A 2010 report from the Center for
Strategic and International Studies con-
cluded that there are only about 1,000
individuals in the United States with
the specialized security needs to defend
cyber space, whereas 10,000 to 30,000
are needed. The reasons for this dearth
of talent include a lack of interest in
pursuing science, technology, engineer-
ing and mathematics (STEM) majors in
college; poor salaries when compared
to the private sector; and complex secu-
rity clearance processes.
Another, often less-recognized reason
is confusion over the value of certifi-
cations. That’s why one of the initiatives
from the nation’s National Initiative for
Cyber Security Education, to be led by
the Office of Personnel Management, an
independent branch of the federal gov-
ernment charged with managing civil
service, is trying to create a common
taxonomy for cyber security profession-
als that will enable hiring agencies to
match roles to competencies.
C3, in conjunction with the Univer-
sity of Maryland and several analytics
firms, is planning to embark on a study
on behalf of the U.S. Homeland Secu-
rity and Defense departments that will
measure the value of certifications, both
for the individual who takes the exam
— remember, there are months, some-
times years of preparation required —
and the organizations who employ the
certified workers.
Adjusting for the times
Clearly, demonstrating the value
of certifications is a key priority for
credentialing bodies. Regardless, the
flagship accreditations are doing better
than ever. Tipton says D ecomber was
a record-breaking month, when there
were some 3,700 CISSP exams taken
(only about half passed).
And it’s no surprise that it is one of
the most sought-after certifications,
considering holders make about $98,000
a year on average, up from $78,000 if
they didn’t have it. (ISC)², which also
offers well-known designations like the
Certified Secure Software Lifecycle Prof-
essional (CSSLP) and Systems Security
Certified Practitioner (SSCP), counted
more than $25 million in assets in 2010.
T he allure of acronymic designations
extends to specific products as well, as
says Tony Iovinelli, president of West
Chicago, Ill.-based SmartSource, an IT
staffing company. H e is firm hires person-
nel for tech clients, which then out-
sourcing these workers to organizations in
need of someone certified, for example, a
Cisco Gold partner.
“It could be that the vendor is
upselling that they have certi-
fied people,” says Iovinelli. “But
there’s a reason they do it.”
or it could be the buyers are being more demanding,” Iovinelli says. Either way, a certification embodies dedication, “it gives them comfort when hiring individuals,” he says. “If this individual went through that certification process with a vendor, the certifications kind of screen their willingness to improve their own skills and character.”

Still, the value of certifications is dropping, according to Veron Beach, Florida-based Foote Partners, which tracks the market. In fact, their value, defined as the portion of a worker’s salary tied to the individual carrying a credential, dropped nine percent over the last two years.

David Foote, the company’s CEO, says 2013, in particular, was a correction year for certifications. As budgets sprung back to life following the financial collapse of 2008, organizations became more focused on investing in revenue-generating projects, something security oftentimes fails to provide.

“[Certifications] are not as important as they used to be in the overall template of what a security person is,” Foote says. “Now they’re influencers, they’re marketers, they’re evangelists.”

The most desired security hire has become those individuals who can show off multidimensional talents, specifically their ability to connect with the business and speak the language, Foote says. As a result, employees with a narrower, technical focus – and their related certifications – get short shrift.

“We help security was thought of as more of a technical issue, security certifications were much more popular,” Foote says. “People have realized you can’t have – or are going to be – hit by adversaries. That’s why he says they need to have security employees who are well versed in the admittedly less glamorous position of defense.

“We’re good at deconstructing things,” says Piscitello, “We’re not quite as good at constructing things that don’t break. So it might be nice if we concentrated on that aspect when teaching people.”

Part of that includes building a network and communications channel that enables trustworthy incident response, he says, adding that he could never envision hiring a convicted hacker. “Part of the fundamental problem here with the way we’re approaching this is we’re starting off with the boundaries that we want people to be creative and explore, but we don’t give them boundaries. (ISC)’s Tipton says he believes certifications provide the best way to validate one’s skill set. In fact, when he began in 2002 at the Department of the Interior, Tipton remembers entering a culture where there was little, if any, concern paid to an adversary who may want to steal data. But eventually, the mindset changed, and certifications were a big part of driving that shift. Tipton remembers his boss determining that the best way to vet the security abilities of its staff was to have members take the CISSP. The agency gave them a year to prepare, and despite “a lot of screaming and hollering” by workers, it turned out to be the best decision.

“I wound up being the first CIO in a Cabinet-level job to get it,” says Tipton, who is not related to the recently deceased H arold “Hal” Tipton, who co-founded (ISC)2 in 1989. (The organization also lost another long-time staffer in March when Judy Livers, senior market development manager, passed away.)

Still, he admits that while taking certification exams requires training and meets educational needs that many colleges and universities currently can’t provide, it is no substitute for more formalized learning.

That’s why (ISC)’s charitable arm, the (ISC)2 Foundation, is trying to reach students before they arrive at college, with efforts such as its Safe and Secure Online program, which encourages professionals to visit 3- to 14-year-olds at school and get them interested in the field. The program also offers scholarships to high school students who excel in capture-the-flag competitions, such as the U.S. Cyber Challenge.

“Education across the board is desperately needed,” Tipton says. “Our quest is to get this to high school, where people can be trained on this on the ground up and don’t have to be converts from other areas. Our academic systems are not designed to develop people like this as they might be for hard sciences.”

**CISPP:**

**Tests 10 domains**

- Access control
- Telecommunications and network security
- Information security governance and risk management
- Software development security
- Cryptography
- Security architecture and design
- Operations security
- Business continuity and disaster recovery planning
- Legal, regulations, investigations and compliance
- Physical security

**What’s Your Next Career Move?**

The information security field is growing and maturing rapidly: are you positioned to win?

A Master’s Degree in Information Security from the SANS Technology Institute will help you build knowledge and skills in management or technical engineering.

**STI offers two unique master’s degree programs:**

**Master of Science in Information Security Engineering**

**Master of Science in Information Security Management**

In addition to course work, STI offers students a unique opportunity to learn leadership skills, share knowledge and research with the information security industry, and build a solid network of peers.

“The STI program prepares me in both technical aptitude and leadership skills. The instructors have extensive real-world experience – you walk out of every class with skills you can use immediately.”

-COURTNEY IMBERT, MSISE Student

Enroll by August 1, 2012 to be eligible for a scholarship of up to 30% of your first year’s tuition.
A selection of some of the schools offering information assurance programs recognized by the NSA and DHS.

Some 120 U.S. universities have been designated by the National Security Agency (NSA) and the Department of Homeland Security (DHS) as Centers of Academic Excellence in Information Assurance (IA) and/or Research. We sent out questions to all schools noted for their strong IA programs, seeking details about their offerings and more. From this feedback, we’ve compiled a listing of some of the universities that shared additional insight.

California State University, San Bernardino
Which degrees/certificates are offered?
B.S., information assurance and security management; M.B.A., information assurance and security management.
What roles/jobs do your students enter upon graduation?
Many students have found positions within government (county, state and federal) and industry (supply chain).

Cal Poly Pomona
Which degrees/certificates are offered?
B.S., information assurance and security management; M.S., degree in computer and information security.
What roles/jobs do your students enter upon graduation?
Finance, government, software and technology companies.

Capitol College
Which degrees/certificates are offered?
We offer 12 B.S. degrees, six M.S. degrees, one M.B.A. degree, and one doctor of science degree. Of these, three degree programs (B.S., M.S., and doctor of science) are offered in the field of information assurance (IA). Capitol College also offers 10 undergraduate certificates and six post-baccalaureate certificates.
What roles/jobs do your students enter upon graduation?
Many of our students are currently employed or seek employment in the Department of Defense, including the supporting contracting community. Capitol College’s physical location near Department of Defense agencies and contractors position us well to help students gain entry into these competitive fields.

Carnegie Mellon University
Which degrees/certificates are offered?
The Information Networking Institute (IN2) offers M.S. degrees in the following areas: information assurance (Eexcel M.S.), M.S. in computer science, M.S. in software engineering, M.S. in computer networking and information security.
What roles/jobs do your students enter upon graduation?
Our students in our program are very well positioned to enter the job market in a variety of roles related to information assurance and cyber security.

Colorado Technical University
Which degrees/certificates are offered?
Computer security is a major focus for our computer science degree programs. We have a B.S. in computer systems security, an M.S. in computer science with a concentration in computer systems security, an M.S. in management with a concentration in information systems security, and a doctor of computer science with concentrations in both digital systems security and information assurance.

Champlain College
Which degrees/certificates are offered?
B.S. in computer and digital forensics, B.S. degree in computer networking and information security, M.S. degrees in digital forensics management (this is an online degree), M.S. degree in digital forensic science (this is an online degree).
What roles/jobs do your students enter upon graduation?
Our students enter into a number of fields across industry, government and academia.

Dartmouth College
Which degrees/certificates are offered?
B.S., M.S. and Ph.D. in computer science.
What roles/jobs do your students enter upon graduation?
Our graduating students enter into a number of fields across industry, government and academia.

Georgia Institute of Technology
Which degrees/certificates are offered?
The Georgia Institute of Technology offers a focused M.S. degree in information security. This is a technical degree program suitable for students who already have a strong understanding of computer science, and it is available at our Atlanta campus or via distance learning. Students enrolled in our more general M.S. degree in computer science can choose to specialize in information security.

Jacksonville State University
Which degrees/certificates are offered?
B.S. in information assurance and security management.
What roles/jobs do your students enter upon graduation?
Our students tend to get jobs designing and implementing security. Major employers of our students include government and industry.

Mississippi State University
Which degrees/certificates are offered?
We offer B.S./M.S./Ph.D. in computer systems and information assurance concentration.
What roles/jobs do your students enter upon graduation?
Software engineer, computer security professional, network administrator, database administrator, system analyst.

Ohio University
Which degrees/certificates are offered?
M.S. in information assurance.
What roles/jobs do your students enter upon graduation?
Our students enter into a number of fields across industry, government and academia.

The George Washington University
Which degrees/certificates are offered?
We offer the following: graduate certificate in computer security and information assurance (CSIA), which requires the successful completion of four graduate courses in computer security; M.S. degree in computer science, which allows students to select several cyber security courses as an area of focus; a Ph.D. degree, which allows students to acquire knowledge and conduct research in several areas, including security and in other areas of computer science; a B.S. degree and a B.A. degree, both in computer science, which require a student to take a technical track.

Special section: Education

IN SESSION

A selection of some of the schools offering information assurance programs recognized by the NSA and DHS.
science and/or technology applications; graduate degree: M.S. in information systems and security (this is an online degree).

New Jersey City University
Which degrees/certificates are offered?
B.S. and M.S. degrees in national security studies. Additionally, NJCU has been authorized by the National Security Agency and U.S. Department of Homeland Security to offer and issue two certificates: Information systems security professionals, NSTISSI 4011, and information systems security officers, CNSSI 4014. These certificates are typically completed within the B.S.-4011 and M.S.-4014E, but can be completed independently if a student already holds a related bachelor’s degree (for 4011) or master’s degree (4014E).

New Jersey Institute of Technology (NJIT)
Which degrees/certificates are offered?
M.S. in cyber security and privacy. What roles/jobs do your students enter upon graduation? The program prepares graduates for job titles such as: information security engineer, network security engineer, network security architect, systems and software security engineer, security analyst, computer/network security consultant, computer security specialist.

Norfolk State University
Which degrees/certificates are offered?
B.S. in information assurance; B.S. in computer security and information assurance. Can you provide a basic rundown of the tracks/courses offered? At the bachelor’s level, we have three available concentrations: digital forensics, information warfare and advanced information security.

Nova Southeastern University
Which degrees/certificates are offered?
M.S. degree programs: computer information systems, information technology in education, information security, information technology management, information technology systems. Ph.D. degree programs: computer information systems, information systems. Graduate certificates in administration of information security and information security systems.

Ohio State University
Which degrees/certificates are offered?
Computer science: bachelor’s degree; master’s degree; two information assurance graduate certifications. What sectors are students prepared for? Graduates are sought out by agencies across all levels of government and by all sectors of the corporate infrastructure, both public and private.

Missouri University of Science and Technology
Which degrees/certificates are offered?
Graduate certificates in software design and development, multimedia and information systems, wireless networks and mobile systems, and information assurance and security officer essentials certificate; B.S. in computer science; M.S. in computer science; Ph.D. in computer science.

Rochester Institute of Technology
Which degrees/certificates are offered?
B.S. in information security and forensics, B.S. in applied networking and system administration, M.S. in computer security and information assurance. Advanced certificate in information assurance, advanced certificate in networking and systems administration, advanced certificate in network planning and design.

Southern Methodist University
Which degrees/certificates are offered?
M.S. in security engineering, graduate certificate in information systems security, M.S. and Ph.D. in computer science, M.S. and Ph.D. in computer engineering.

State University of New York, Buffalo
Which degrees/certificates are offered?
Advanced graduate certificate in information assurance. Can you provide a basic rundown of the tracks/courses offered? Fundamentals of programming languages operating systems internals computer, communications database systems computer security, wireless networks security, modern networking concepts data mining applied cryptography and computer security, digital forensic database management systems system analysis and design information assurance, network management, seminar in e-commerce, intellectual property, law, legal and cultural issues in cyber space.

Pace University
Which degrees/certificates are offered?
Pace students have the opportunity to complete a minor or a career focus/concentration in information assurance. Pace also offers information assurance-related certificates at the undergraduate and graduate level. Advanced certificates are offered in security and information assurance, secure software and information engineering.

Get a master’s in homeland security with a focus on information security and forensics.
- Prepare for challenging leadership positions
- Develop critical skills in information systems and cyber security
- Fit a degree program into your life with the online learning format
- Expand your professional network with classmates and faculty
- Earn a Postbaccalaureate Certificate in Information Systems Security along the way

Learn more about Penn State’s online information security programs and request additional information.

Achieve your career goals—apply today!
www.worldcampus.psu.edu/SCMag12
University of Advancing Technology
Which degrees/certificates are offered?
B.S. in network security, B.S. in technology forensics, master’s in information assurance.
Can you provide a basic rundown of the tracks/courses offered?
Network security, digital forensics, master’s in information assurance.

University of Alabama, Huntsville
Which degrees/certificates are offered?
M.S. in information assurance and security – multidisciplinary; graduate certificate in information assurance; M.S. in engineering in electrical engineering/computer engineering (concentration in information assurance); Ph.D. in EEE/CPE.

University of Arizona, Tucson
Which degrees/certificates are offered?
B.S. in computer science, M.S. in computer science, Ph.D. in computer science.
Which degrees/certificates are offered?
M.S., Ph.D. in information assurance. The Center of Excellence for each student specializing in information assurance (IA) certificate programs both at the undergraduate and graduate levels. In addition, we offer a minor in IA for non-computer science majors. Finally, we offer a graduate level concentration track in IA for M.S. or Ph.D. students pursuing degrees in computer science.

University of California, Irvine
Can you provide a basic rundown of the tracks/courses offered?
These are security-centered courses. There are many others that touch on security: foundations of cryptographic protocols; applied cryptography; network and distributed systems security; and language-based security.

University of Detroit, Mercy
What roles/jobs do your students enter upon graduation?
A list of public and private sectors.
What year did you receive NSA designation?
June 2009

University of Idaho
Does your program offer any scholarships?
In 2001, the National Science Foundation began funding the University of Idaho’s Scholarship for Service CyberCorps, which pays up to $35,000 per year for each student specializing in information assurance. The Center of Excellence designation and CyberCorps funding have been renewed every three years and are still in place today.

University of Illinois at Springfield
Which degrees/certificates are offered?
We offer B.S. and M.S. in computer science. Can you provide a basic rundown of the tracks/courses offered? We offer an emphasis on software engineering and an emphasis in systems security and information assurance.

University of Illinois, Champaign-Urbana
Which degrees/certificates are offered?
M.S. in computer science; M.S. in information sciences; Ph.D. in computer science; Ph.D. in information assurance.

University of Kansas
Which degrees/certificates are offered?
B.S. in electrical engineering, computer engineering, computer science, and inter-disciplinary computing. M.S. in electrical engineering, computer engineering, computer science, and information technology. Ph.D. in electrical engineering, and computer science.

University of Kentucky
Which degrees/certificates are offered?
M.S. in computer science; M.S. in information sciences; Ph.D. in computer science; Ph.D. in information assurance.

University of Maryland, Baltimore County (UMBC)
Which degrees/certificates are offered?
B.S., M.S., Ph.D. in computer science. B.S., M.S., Ph.D. in computer engineering. M.S., Ph.D. in electrical engineering. B.S., M.S., Ph.D. in information systems. M.S. in cyber security. Graduate certificate in professional studies: cyber security strategy and policy.

University of New Mexico (UNM)
Which degrees/certificates are offered?
B.S. in computer science, M.S. in computer science, and a Ph.D. in computer science.

University of Oklahoma
Which degrees/certificates are offered?
M.A. in computer science; M.S. in computer science; Ph.D. in computer science.

University of Oregon
Which degrees/certificates are offered?
B.S. in computer science; M.S. in computer science; Ph.D. in computer science;

University of Pennsylvania
Which degrees/certificates are offered?
B.S. in computer science; M.S. in computer science; Ph.D. in computer science.

University of Portland
Which degrees/certificates are offered?
B.S. in computer science; M.S. in computer science; Ph.D. in computer science.

University of Rhode Island
Which degrees/certificates are offered?
B.S. in computer science; M.S. in computer science; Ph.D. in computer science.

University of South Carolina
Which degrees/certificates are offered?
B.S. in computer science; M.S. in computer science; Ph.D. in computer science.

University of Tennessee at Chattanooga
Which degrees/certificates are offered?
B.S. computer science – information security and assurance; M.S. computer science – information security and assurance. We also offer certificates in advanced information systems security and information systems security.

University of Texas at Dallas
Which degrees/certificates are offered?
Our program is housed within the computer science department and we offer information assurance (IA) certificate programs both at the undergraduate and graduate levels. In addition, we offer a minor in IA for non-computer science majors. Finally, we offer a graduate level concentration track in IA for M.S. or Ph.D. students pursuing degrees in computer science.

University of Washington
Which degrees/certificates are offered?
The Center for Information Assurance and Cybersecurity (CIAC) is a multidisciplinary center drawing from different degree programs across the University of Washington. This includes master’s and Ph.D. programs in electrical engineering, computer science, and engineering. Mathematics and more. The master’s in information management in the information school includes an information assurance/security specialization track.

Assurance on the Shore

A New Jersey public school system found a way to serve increasing broadband needs, while protecting its network, reports Greg Masters.

Rick is a township on the central New Jersey coast which is bordered on the east by three beaches. A N inlet, Kingtons Cove, splits the topography down its middle before emptying into the Atlantic Ocean. While decades ago it was primarily an agricultural area, following development of the Garden State Parkway in the 1950s, the region has become a popular destination for summer vacationers. Almost hourly, trains on the New Jersey Transit’s North Jersey Coast Line shuttle passengers between Penn Station in midtown Manhattan and the next town over from Brick, Bay Head, a 2½-hour scenic ride that includes stops in Asbury Park and Point Pleasant.

Brick’s year-round residents enjoy a quiet atmosphere that – despite the incursion of chain stores and fast-food restaurants – still maintains an aura of the 1950s, with kids riding their bikes on rural streets canopied with trees that are generations old. In fact, in a 2006 survey extrapolated from FBI statistics, the town was cited as one of the safest places to live in the United States (though the FBI has since refuted the use of its crime statistics in compiling quality-of-life charts). The township has a population just more than 75,000, according to the 2010 census, and the school district serves 10,000 students in pre-kindergarten through 12th grade. While the environs might make some nostalgic for a more bucolic time, the majority of the population has been swept along like everyone else into the 21st century, keeping up with the latest gadgets and electronics. And, with the explosive growth of digital
special section: education

namely sports, where visitors, coaches,
In addition, there are off-hours events,
ing the network's internet bandwidth.

devices. This strategy was deteriorat-
he terms an "iGarbage bin" of wireless
music and video websites, like Pandora,

Websites," Ellicott says. "Simultaneous-
rich interactive- and multimedia-based

curriculum], YouTube teaching and
[test preparation software programs]
education sites, such as Study Island

being transmitted.
traffi c on the school district's network,

engorged

was a priority. He went looking for a solu-

ellicott, manager of network opera-

media personnel and other guests
require internet access.

As a result, bandwidth was and still is
off the charts, and we found that our fire-
walls were no longer sufficient," he says.

Other challenges
But increasing speed and availability on
the network was not the only priority.
Ellicott and his team faced other chal-

enges as well. Of most concern was that
cyber threats have increased.

A cyber criminals can now hack into
the network from the application level,
the district found that first-generation
firewalls were not sufficient to deal with
the emergence of application-based
threats, says Ellicott.

Is a team found there were many false
positives, as cyber criminals managed
to send emails that looked legit, but
weren’t. Eventually, they had trouble
detecting which threats were real and
which weren’t, plus schools throughout
the district had difficulty logging into
the network to complete their work or
lessons. These and other problems threw
the day-to-day operations of the school
system into chaos - causing his raid or
work 24/7 to try and resolve the issues.

“Basically, stateful firewalls [a fire-
wall programmed to keep track of net-
work connections so as to differentiate
legitimate packets for various connec-
tions and block those that don’t match
a known active connection] to me are
dead,” he says. “The attacks that are
happening today are emanating from
within and going out. It’s all botnets
and rogue applications now. People try
to lure you into clicking on an email, or
you pass by a website infected by a virus
and you get rogue anti-virus and rogue
pop-ups.”

And, his team found that most intru-
sions were arriving with people using
mobile devices. This was particularly
alarming as there are technical concerns
unique to the education sector. Ellicott’s
team wondered how these devices were
being used. A surveying that most users
were students, the question for his team
was: How does an unnoticed Droid or
iPhone assist in a test-taking scenario?

Elicit and his team faced other chal-

lenges as well. Of most concern was that
cyber threats have increased.

A cyber criminals can now hack into
the network from the application level,

the district found that first-generation

firewalls were not sufficient to deal with

the emergence of application-based

threats, says Ellicott.

A safe, secure and fast network
The Brick Township school district has
five full-time members on its IT team,

who are working to provide security that
enhances productivity." - Ross Ellicott, Brick Township Public Schools

UPDATES: Keeping current
SonicWALL customers with active security
services, such as the Brick Township public
school district, receive regular updates by
the firewall polling the company’s back-end
servers, says Dmitry Ayrapetov, product
line manager of network security at the
San Jose, Calif.-based provider of internet
security solutions. Usually the updates are
hourly, but in some cases can become more
frequent. There are no reboots necessary

when an update is applied.

Additionally, the company’s cloud-assist
anti-virus feature, called Cloud-GAV, allows
the firewall to query an additional six mil-

lion-plus malware signatures that exist on
the backend, Ayrapetov says. The updates
there, by definition, are instantaneous.
“Most organization at this point are
extremely aware of the benefits of deep
packet inspection, but we’ve seen most
avoid deploying this technology because
of performance implications or because
of negative experiences with vendors who
focus on protecting just a few common
ports,” says Ayrapetov.

“Our vision is to eliminate this per-
formance concern and to reassure our
customers that all ports are protected;
and administrators can regain control of
their networks even if all applications start
streaming over HTTP,” Ayrapetov says.

“We give them this visibility without a sac-
ifice in performance. Security gets turned
off if it hinders productivity and work,
and we are working to provide security that
enhances productivity.”

- GM

Cyber criminals were able to penetrate the network...

- Ross Ellicott, Brick Township Public Schools

Success Starts Here

Information Assurance with Iowa State University

You Are the Future

Your success is directly proportionate to the
investment you make in yourself...in your education.

At Iowa State, we give you many options to reach your
goals by offering graduate, certificate, and professional
development programs to best suit your needs.

Make it work for you—we offer 100 percent online
degree programs to help you advance your knowledge
and your career.

Join a program at the beginning of any semester and
take graduate courses in any order at a pace that suits
your schedule.

We Are the Leader

U.S. News & World Report recognizes Iowa State’s College
of Engineering as one of the nation’s leading providers of
online graduate education.

The National Security Agency named Iowa State one of
seven charter Centers of Academic Excellence in Information
Assurance Education in 1999.

Over one-third of our online courses have hands-on lab
experiences, including an information assurance capstone
course where you design, build, and defend a network.

Iowa State boasts one of the largest information assurance
educational degree and certificate programs in the nation
as well as faculty with national reputations as leaders in
computer security.

We also offer corporate training—Prepare your staff by
providing the tools they need to be your frontline defenders.
We offered specialized security training for corporate IT staff and
security literacy training for all staff.

For more information about our degree programs
and specialized corporate training in information
assurance, visit www.iol.iastate.edu/infas or contact us
at infas@iastate.edu or 515-294-0659.
in addition to E11cott — a director, web and help desk personnel; and two building-level technicians. Two part-time employees are available for building-level work as well.

The district connects 3,500 devices, including 1,500 IP phones, across 16 building locations. E11cott says. In addition, there has been a big increase in staff and students connecting to the network using iPhones and Android mobile devices. Prior to upgrading the school district’s internet bandwidth, his team had no choice but to shut down its guest wireless network. What the Brick IT team originally thought would be a few guests, in fact ballooned to more than 500 registered devices.

Brick, he says, is a large school district trying to help its teachers and students take advantage of interactive and web-based learning technologies and tools. “We needed a solution that could provide our staff and students with a safe, secure and fast network,” he says.

The search begins

E11cott and his boss — Leonard Niebo, the director of technology — reviewed a number of solutions to alleviate the congestion on Brick’s network. Time was of the essence, so there was not a long evaluation period. The first tool they examined lacked an efficient management interface. One firewall they judged to be less intuitive lacked a full range of features and came with a frustrating performance security engine, he adds. A critical aspect of the engine is that it can scan everything, regardless of the type, and that results in a high-latency approach is combined with a multicore processor, and that results in a high-performance security engine, he adds.

“By not proxying connections, like most other competitors do, we can scan hundreds of thousands of network streams of unlimited size simultaneously without introducing latency through buffering,” says Ayrapetov. This approach is combined with a multicore processor, and that results in a high-performance security engine, he adds.

Two SonicWALL E6500s now sit in the school district’s core server room with redundant WAN links. It also has a SonicWALL NSA 2400 at high-population, low bandwidth for internet egress. And, E11cott says, his team is now working to complete a site-to-site virtual private network (VPN) to a remote warehouse, primarily to connect the new voice over IP (VoIP) phone network. They are also working to complete its Active Directory-aware, user-based access controls.

“We cater to children through adult,” E11cott says. “High school students are crafty and keep our department on its toes, while staff requires greater security and access to different computing platforms. We have a great responsibility to protect not only adults in the district but children as well.”

SC May 2012 www.scmagazine.com

Special section: Education

For deep-packet inspection,” says Dmitriy Ayrapetov, product line manager of network security at SonicWALL, which has its U.S. headquarters in San Jose, Calif. (Dell acquired the company in March for, it is believed, around $1.2 billion.)

The district has since deployed paired SonicWALL E-Class Network Security Appliance (NSA) E6500 Next-Generation Firewalls in high availability (HA) mode, running SonicOS 5.8, and bundled with SonicWALL TotalSecure. In addition to freeing up bandwidth to accommodate the increase in users and the amount of data being transmitted, the solution also provides gateway anti-virus, anti-spyware intrusion prevention, application intelligence and control, content filtering, firmware updates and 24/7 support.

SonicWALL products differ by their design philosophy, which is based around a single-pass streaming inspection engine that does not rely on proxies for deep-packet inspection,” says D. Dmitriy Ayrapetov, product line manager of network security at SonicWALL, which has its U.S. headquarters in San Jose, Calif. (Dell acquired the company in March for, it is believed, around $1.2 billion.)

The district has since deployed paired SonicWALL E-Class Network Security Appliance (NSA) E6500 Next-Generation Firewalls in high availability (HA) mode, running SonicOS 5.8, and bundled with SonicWALL TotalSecure. In addition to freeing up bandwidth to accommodate the increase in users and the amount of data being transmitted, the solution also provides gateway anti-virus, anti-spyware intrusion prevention, application intelligence and control, content filtering, firmware updates and 24/7 support.

By not proxying connections, like most other competitors do, we can scan hundreds of thousands of network streams of unlimited size simultaneously without introducing latency through buffering,” says Ayrapetov. This approach is combined with a multicore processor, and that results in a high-performance security engine, he adds. A critical aspect of the engine is that it can scan everything, regardless of the type, and that results in a high-performance security engine, he adds.

Two SonicWALL E6500s now sit in the school district’s core server room with redundant WAN links. It also has a SonicWALL NSA 2400 at high-population, low bandwidth for internet egress. And, E11cott says, his team is now working to complete a site-to-site virtual private network (VPN) to a remote warehouse, primarily to connect the new voice over IP (VoIP) phone network. They are also working to complete its Active Directory-aware, user-based access controls.

“We cater to children through adult,” E11cott says. “High school students are crafty and keep our department on its toes, while staff requires greater security and access to different computing platforms. We have a great responsibility to protect not only adults in the district but children as well.”

The current need for trained information assurance professionals in government and industry is significant and will continue to increase. Northeastern’s MSIA program will help you become a trained IA leader.

• Learn how to make strategic decisions about information security issues including: identity theft, computer viruses, and electronic fraud

• Combine IA professional training with practical exercises taught by industry experts with 20+ years of experience

• Take technical and contextual courses tailored to your background

Complete your degree in as few as four semesters—100% online, on campus, or by mixing the formats.

Learn more at http://pages.northeastern.edu/MSIA 1.877.634.6865

Northeastern University
Degree programs are valuable, but some say that the IT field is moving so fast that graduates might be at a disadvantage, reports Alan Earls.

Experts see a chasm between the personnel needs in the information security field and the numbers of skilled people available to fill those needs. However, they also believe that more needs to be done in the area of higher education to help fill the gap.

“The gap is general,” says Peter Stephenson, director of the Norwich University Center for Advanced Computing and Digital Forensics, and an associate professor and chief information security officer at the school. “There are thousands of information assurance jobs that go unfilled every year,” he says, adding that a gap exists in both the private sector and in government. “It’s not limited to any one sector, we are simply not turning out enough qualified graduates.”

In fact, there are a growing number of programs nationwide that focus on IT security and forensics. At issues is whether they are expanding fast enough and whether more needs to be done to attract and motivate students.

“We sometimes joke that we need a television show like CSI to make these jobs more attractive,” says Constance Knap, the interim dean of Pace University’s Seidenberg School and a co-director at the Seidenberg Cyber Security Institute. “We want all we need to do is to talk up the career opportunities, to make it clear that the need for these jobs will increase over time and that there is an acute shortage now,” she says.

One of the efforts to bolster higher education has been the Center of Excellence designations, supported in part by the Defense (DoD) and Homeland Security departments (see list of schools on page 26). Stephenson, for one, helped establish the Eastern Michigan University Information Assurance Program Center of Academic Excellence in Information Assurance, which was sponsored by the National Security Agency. He also helped Norwich set up a pilot Center for Digital Forensic Academic Excellence program – one of eight colleges so designated by the DoD Cyber Crime Center.

However, just because a school is a Center of Excellence doesn’t mean it has a comprehensive program, says Stephenson, who is also technology editor of SC Magazine. “The problem with centers of excellence is that the field has become so broad that universities can’t afford to cover all the territory, so they try to specialize,” he says.

Derek Thomas, an information security consultant at Auburn Hills, Mich.,-based security solutions provider Vipoint, is a recent product of security-oriented higher education. He says he chose the field because it always fascinated him. “I read there was a surge in network security-related positions and that it was slated to grow for many years to come,” he says.

Also, the relationship that an institution has with prospective employers could help draw people into the infosec field, he says. “I believe that programs should educate students on what types of jobs will be out there for them,” he says. “I didn’t know what jobs I could qualify for as a grad without any professional experience.” However, he now believes employers are looking for candidates who can show not only their degree but also specialized certifications and proof that they are driven to excel in their field.

“I believe the problem with education is that when we teach our students we want to teach them both information security and business, but the two of them aren’t really intermingling or intertwining,” says Damon Petraglia, owner and director of forensics and information security services at Chartstone Consulting in Stratford, Conn.

In the future one won’t be able to process information without having security, but the two topics are still taught separately, Petraglia says. “When I teach a class, I have almost entirely IT students, not business students, so I think the curriculum needs to change to engage both,” he says.

Has your organization hired individuals specifically for information security roles?

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not sure 8.4%</td>
<td>No 19.6%</td>
</tr>
<tr>
<td>Yes 72%</td>
<td></td>
</tr>
</tbody>
</table>

How difficult has it been to find the right candidate(s)?

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not difficult at all 6.1%</td>
<td>Very difficult 29.3%</td>
</tr>
<tr>
<td>Somewhat difficult 50%</td>
<td>Haven’t begun the search yet 14.6%</td>
</tr>
</tbody>
</table>
Before moving assets to the cloud, CISOs must determine how much security they’re willing to contract out, reports Stephen Lawton.

Cloud security inherently is no better or worse than what is in place at corporate data centers, says Aider’s Westby. "If the cloud is secure?" he says, the executive should ask if use of the cloud is secure. And that is because cloud providers look at security differently than do their customers. Companies should take nothing for granted when selecting a cloud provider, he says. "You can’t assume [the provider] has an intrusion protection system (IPS) in front of its servers," Chuvakin says. Nor that any IPS that a provider does have will be sufficient for the client’s required level of security. If a cloud provider is unable to guarantee a company that it can meet its needs, or that the level of protection required could be prohibitively expensive, the customer always has the option to choose a different approach, such as a private or hybrid cloud.

Before choosing a cloud provider, Chuvakin recommends the security manager determine whether he or she has the confidence that the provider has the technical wherewithal to secure the hypervisor - the system that allows various operating systems to run at the same time on a host computer. If the client’s data will be on the same physical server as other clients’ virtual servers, then the security officer requires absolute assurances that the provider can protect the hypervisor. If a hypervisor is breached, an attacker can compromise and gain access to all of the other tenants on the same server.

A more extensive version of this article is available on scmagazine.com.
About 24,000 Medicaid patients in Utah got word in early April they’d have to check their credit and bank statements for fraudulent activity much more diligently after hackers breached a Utah Department of Health (UDOH) server storing thousands of their records. Then, a couple of days later the news became much worse when the still-continuing investigation uncovered that Children’s Health Insurance Plan (CHIP) recipients also were affected.

The tally of client records removed by cyber criminals from the server currently stands at 780,000. Of those, some 280,000 patients have seen their Social Security numbers compromised. 280,000 patients have seen their Social Security numbers compromised. An average of 200,000 individuals were affected. This year, some 31 incidents have already been reported.

As the investigation is still underway, the UDOH breach hasn’t made that list just yet. But, some information has been released. The Utah Department of Technology Services (DTS) initially thought 24,000 claims were affected by the attack. It turns out, however, that one of those files can contain claims on hundreds of individuals. And the kinds of information often found on these include Social Security numbers, addresses, tax ID numbers, doctors’ names and more.

Also early on in the investigation, it was stated that the cyber criminals believed to have accessed a server out of bounds with normal procedures as the primary culprit. “DTS has identified where the break-down occurred and has implemented new processes to ensure this type of breach will not happen again,” according to a UDDH press release. “Additional steps are being implemented to improve security controls related to the implementation of computer hardware and software, as well as increased network monitoring and intrusion detection capabilities.”

However, some professionals at the SC Magazine Roundtable likely would have contended that had proper risk management protocols, such as regular risk assessments and external audits, been established and put into practice, such server misconfigurations and any resulting brand-damaging breaches may have been avoided.

Currently, there is a gigantic dearth of risk assessments being undertaken. Contino said at the SC Magazine roundtable, it is such documented and objective risk barometers could assist organizations in keeping plans updated, as well as help them prioritize security needs. According to a recent Health Care Information and Management Systems Society (HIMSS) survey of large health care organizations, 47 percent conduct annual risk assessments and this is despite the fact that these are a required note in the original HIPAA security mandates.

One problem may be lingering budget issues, said Richard Kaplan, a senior security consultant with Open Sky, who attended the event. To undertake activities such as these, money is needed, but it is only the office tasked with enforcing the Health Insurance Portability and Accountability Act (HIPAA), which is part of the economic stimulus package known as the American Recovery and Reinvestment Act of 2009.

Starting the breach incidence count with the inception of HITECH and its data breach notification requirement that first year, the civil rights office reported from September to December 2009, which affected about 2.4 million individuals. Come 2010, the number of breaches jumped to 259 with 5.4 million individuals exposed. Last year, 147 incidents were reported, but those affected went well into the millions given that a few organizations alone saw huge exposures, including TRICARE at 4.9 million individuals exposed. Last year, 147 incidents were reported, but those affected went well into the millions given that a few organizations alone saw huge exposures, including TRICARE at 4.9 million individuals exposed.

While sometimes accepting a level of risk associated with a business deployment is a common practice among health care entities, adhering to IT security best practices and implementing technologies still is not for some organizations.

The challenge is that we’re going to need more and more security as we go forward,” said Contino. “Yet the conversations at the C-suite level tend to be about other priorities. So I guess the question is how do we elevate the security discussion so that [executives] realize [security] goes hand in hand with all the technologies being implemented. Without it, we’re creating enormous risks for our institutions.

There are more organized hacking attempts that are confronting health care now.”

Paul Contino, CTO at New York City HHC
Compliance Week 2012 will feature sessions with federal officials, regulators, standard setters, enforcement officials, and, of course, chief compliance officers. Don’t miss this critical event.

Special SC Magazine subscriber rate of $1,895 [use code CW12SCMG7]
Register today at: conference.complianceweek.com or call 888-519-9200
SESSION SPOTLIGHT: Stressed! How to Stay Sane in the Modern CCO Job
A recent survey found that 60 percent of compliance officers have considered quitting in the last 12 months due to overwhelming job stress. Don’t bail just yet! Attend this session to hear from other compliance officers about why the job has grown so complex, and share steps you can take to stay ahead of the fray and be more productive on the job.

Featuring:
Laura Merten, CCO, Walgreen Co.
Stephen Epstein, Chief Counsel, Ethics and Compliance, The Boeing Company
Patrick Carney, Assistant General Counsel (Ethics), Federal Communications Commission

SPeakers include:
Time Warner Inc.
VP, Assoc. General Counsel & Chief Ethics & Compliance Officer, Kelli McTaggart

PSycHex
Director of Enterprise Risk Management, Frank Forile

SafeWay Inc.
VP, Financial Compliance, Bill Spoehr

Johnson Controls
Vice President Compliance, Mark Koczela

The Mayflower Hotel, Washington, D.C.
June 4-6, 2012
The quality of the speakers, the information, the participants, and the overall organization were excellent.”
– KC Turan, VP, Chief Compliance & Ethics Officer, Blue Shield of California

“Highly informative and well-balanced. A great opportunity to share best practices and network.”
– Joann Sochor, VP Corporate Compliance, Bank of Montreal

“Compliance officers converge here every year.”
– David Heller, Chief Compliance and Risk Officer, Qwest,
Prepare for a host of new networking problems as devices never meant to be computers become network connected, reports Deb Radcliff.

For example, the health care industry has long used divergent networks to run biomedical devices, like radiology systems, attached to a hospital’s campus network. This equipment is not subject to the same security management requirements as other patient systems because of different regulations, says Barbara Filkins, a security consultant specializing in health care.

W hat’s new, she says, is that many devices used to collect data on a patient’s condition are more mobile and quite possibly employee-owned, which she calls the “makings of a very big risk management problem.”

Connecting the network
These devices have their own connections to a home network, patient systems and emergency services networks, acting as conjoiner of what should be separate networks, Filkins says.

Alarmingly, medical establishments are woefully unprepared for BYOD, let alone the interconnectedness of multiple new medical devices coming online, she says. More than 80 percent of health care organizations allow personal devices in their enterprises, but less than 50 percent of them have any type of security policy around use, according to a recent Ponemon survey.

Extrapolate this to the larger issue of managing devices implanted into humans, says Filkins, and the makings of a nightmare scenario are conjured. “I imagine something like murder by remote-controlled pacemaker,” she says.

H acks on implanted medical devices have already been demonstrated (also at Black Hat 2011) when security researcher Jay Radcliffe sent commands wirelessly to disable his own insulin pump to gain the equivalent of “root” control of that device.

Barnaby Jack, who last year wowed the Black Hat crowd with a talk about ATMs, vulnerabilities, at this year’s gathering also demonstrated how to hack into an insulin pump.

Beyond their personal security, human chip implants pose new challenges philosophically and ethically,” says Will Irace, vice president of threat research at Fidelis Security Systems. “And I don’t have reason to be confident that manufactures design security, let alone understand the new attack surfaces they’re introducing.”

Vendors need to design in better security, say experts, but sometimes laws work against such safeguards. For example, Filkins cites the Food and Drug Administration’s projected move to implement the unique device identification (UDI) standard in 2013, under which all implantable devices would have particular identifiers that would likely include the specific serial number of the device and a MAC or IP address. The ruling is intended to protect users by creating a stronger, more reliable means of reaching and updating connected medical devices. However, these unique addresses will also make them identifiable and a target based on the specific system vulnerabilities, Filkins says.

O ther critical devices, such as controllers, are also easy to identify and therefore target, says Matthew Luallen, who also teaches courses at DePaul University in Chicago and runs the school’s hands-on cyber security and control systems course. Such was the case with Stuxnet, which originally targeted specific Siemens control systems used in Iranian nuclear plants.

L uallen, who also teaches courses through his own company, CY BAT I, has been working with his students to inventory a large and growing number of control systems coming online with vulnerabilities – from amusement park rides to a Japanese bullet train.

“Because these devices are connected, it’s easy to find the specific control systems you’re looking for,” says Lual- len. “In our class, we create Metasploit code [a tool in the Ruby programming language] by which third-party security researchers can investigate potential vulnerabilities.
Networking challenges

Each device using IPv6 will have multiple IP addresses.

— Nancy Jin, product manager, Cisco

Consider also that future devices will likely be IPv6, since IPv4 addresses were fully allocated in February 2012.

“Each device using IPv6 will have multiple IP addresses,” says Nancy Jin, product manager of the wireless networking business unit at Cisco. “This is different from IPv4, and can create challenges with monitoring and visibility.” Distributed denial-of-service (DDoS) attacks are already being carried out through IPv6 traffic, says Jin. If they aren’t already capable of seeing into IPv6 traffic, network management and security systems will need to be upgraded as soon as possible to support this new protocol. Otherwise, as has been proven in many reported examples, payloads can be tunneled in through encrypted IPv6 traffic without any visibility into the threat.

IPv6 network visibility, optimization and acceleration technologies continue to improve to support the massive data and traffic scanning demands today.

Mykons’ Krezet says it’s only a matter of time before the model of deep scanning and inspection into what has come to be called Big Data will no longer scale.

He adds that today’s Big Data monitoring and correlation technologies are not catching advanced persistent threats (APTs), so, he asks, how are they going to handle tomorrow’s problems?

“Smart rooms, white boards, copiers and building control systems can all be connected across a hundred sites, so the benefits of massively simplified management and ease of access to devices will outweigh security concerns,” says Krezet. “That means companies [like juniper] will protect a much larger ecosystem of network types and traffic. To do that, we’ve got to start thinking outside of the box.”

—Peter Stephenson, technology editor

The CSI effect – SC style

Yes, there really is a CSI effect. In the digital forensics program at Norwich University in Vermont, a version of the CSI effect is alive and well. For the third year in a row, students in my computer forensic class have produced this month’s Group Test for digital forensic tools.

Norwich is nearly unique among American universities in that is a Center of Academic Excellence in both information assurance and digital forensics. For this month’s testing, the students team up in pairs and put the tools through their paces and then write the reviews. That is what you now have in front of you, and our hope is that you will enjoy this issue as much as readers have in prior years. What we find most interesting about the students – who work under my close supervision – is that they are really tough reviewers.

The test environment is very complete. There is a lab consisting of 11 Dell forensic workstations, each with twin screens. The lab does not connect to the outside world. Instead, it connects to the virtual clusters that make up the Norwich University Center for Advanced Computing and Digital Forensics virtual lab system, a cluster of four VMware servers.

Hardwire appliances can be installed neatly in the Center with a direct connection into the lab on the two-server cyber weapons range cluster, and traffic can then be generated in the virtual environment so that the network forensic appliances have something to look at.

The end result is that the tools and software really get a worker, and the results in the following pages show that. It was, overall, a very good year for forensic tools.

Because the students were working with me this month, we gave SC Lab Manager Mike Stephenson the month off. The students all are upperclassmen and many are in their last semester. For me, working with these students requires close supervision, but no interference. Also, I want to thank the companies that participated this month. Your products were strong and your support of this new tradition is appreciated.

So, begin this month’s reviews by determining your requirements and then find a product that fits your needs. Some of the products here are sufficiently unique that even if you haven’t planned on buying the particular type of product, you may well start thinking once you see the value.

How we test and score the products

Our testing team includes SC Labs staff, as well as external experts who work for our Group Tests, we look at several products around a common theme based on a predeter-}


The SC Lab environment, and which will be used subsequently in the product's report card. Seriously deficient. An “F” on the product's report card.

We developed the second set of standards specifically for the group under test and use the Common Criteria (ISO 549) as a basis for the test plan. Group Test reviews focus on operational characteristics and are considered at evaluation assurance level (EAL) 1 (functionally tested) or, in some cases, EAL 2 (structurally tested) in Common Criteria-speak.

Our final conclusions and ratings are subject to the judgment and interpretation of the tester and are validated by the technology editor.

All reviews are vetted for consistency, correctness and completeness by the technology editor prior to being submitted for publication. Prices quoted are in American dollars.

What the stars mean

The star ratings, which may include fractions, indicate how well the product has performed against our test criteria.

Outstanding. An “A” on the product’s report card.

Carries out all basic functions very well. A “B” on the product’s report card.

Carries out all basic functions to a satisfactory level. A “C” on the product’s report card.

Fails to complete certain basic functions. A “D” on the product’s report card.

The recognition means

Best Buy goes to products the SC Labs rate at outstanding. Recommended means the product has shine in a specific area. Lab Approved is awarded to extraordinary standards that fit into the SC Lab environment, and which will be used subsequently in our test bench for the coming year.
Digital forensic tools

Today’s forensic tools are characterized by their wide variety of functions, so determining what you need accomplished is key to making the right choice, says Maria Dailey.

Digital forensic tools

We designate NIKSUN NetDetector as SC Lab Approved for another year for its versatility, comprehensive testing capabilities and value.

Technology Pathways ProDiscover is an excellent product streamlined and ideal for collection prior to full investigation. Again this year, ProDiscover is one of our SC Lab Approved products.

Cellebrite UFED Ultimate can be expensive, but it is worth the cost when processing large numbers of mobile devices. It’s excellent for field work as it is fast and easy to use. We make it our Best Buy.

WetStone US-LATT is an excellent product for anyone in law enforcement. Also, it is well worth considering in larger organizations that need to perform triage forensics. We select it as our Recommended product.

Digital forensics is the application of proven methods and investigative procedures for the purpose of reconstruction, reporting and presentation of evidence. It is achieved by preserving original evidence and accurately creating copies for analysis. This discipline is growing in popularity and importance in today’s cyber society. As more devices are introduced to the market, storage for evidence increases, and this growth in the number and variety of electronic media raises a concern in forensic circles. Too, smartphones and tablets are more commonly seen by analysts than PCs in recent years. Databases and networks are not excluded. The integrity and accuracy of the recovered media is completely reliant on the extracting software. Forensic software should consistently produce identical, unaltered copies of digital evidence. This fundamental truth is not restricted to any specific subgroup of forensics. Law enforcement and network administrators alike require that systems analysis should be based on reliable evidence.

Currently, organizations purchase a variety of forensic tools. The main issue is that a single solution that satisfies all needs of an analyst does not exist. A forensic kit targeting computers may not be compatible with cell phones or certain operating systems. Examiners and investigators consequently require additional training due to the variety of forensic software. An ideal solution would be an “all-in-one” product, but oftentimes these kits can consume system resources due to the amount of features offered, some of which may be unnecessary. Specialized kits offer more detail, but limit compatibility. Some kits may be resource-efficient, but leave more to be desired. The challenge for software developers is to find a balance between compatibility, performance and ease of use. Another concern is finding a kit that not only can be used for many devices, but one that can provide for lab and field use. This means the kit must be travel-friendly, accurate and quick to roll out. The following reviews assess the strengths and weaknesses of a variety of today’s forensic tools. We tested products with services for standard digital devices to networks, and a couple specializing in mobile devices, Apple, live system and advanced search. All reviews were based on five points of interest: features, ease of use, documentation, support and value for money. Each tool was individually assessed and graded independent of a competitor’s product tested in the same lab. We compared the functionality against what the manufacturer touted to determine all our judgments. Our mission is to expedite the process of narrowing down consumer choices by eliminating hands-on testing and analyzing whether or not the product suits consumer needs according to its advertised use. Potential users should first know exactly what it is they are looking for in a product. If one currently owns a product which satisfies most needs, consider searching for one that can supplement your primary tool. A nother option is to contemplate whether an all-in-one product would be more beneficial given system specifications. Each product we tested offers focused features and processes ideal for forensic analysis. The final decision lies on the desks of the user. It is unlikely that one product will supply all required capabilities needed for every case. In the race against criminals, choosing the tools fit for the purpose intended is vital. For this Group Test, we took advantage of the skills of the Norwich University computer forensic students under the watchful direction of Peter Stephens. Contributing to this month’s reviews were Timothy Fontana, Ian Hulse, Maria Dailey, Brittney Davis, Darko Poposki, Nicole Chrusciel, Aleksandar Ognenoski, Stephen Resto, Colby LeClerc, Adam Marena, Michael Zemanek, William Griffin, Luna Feiker, Christopher Cummings, Todd Renner and Dejan Stefanoski.

Maria Dailey is a senior computer security and information assurance major at Norwich University and has written articles on information security for several online publications.

Specifications for digital forensic tools

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Live system analysis</td>
<td>Linux compatible</td>
<td>Windows compatible</td>
<td>MAC OSX compatible</td>
<td>Support for custom policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

51
ADF Solutions Triage-Examiner is a forensic tool that scans target devices whether they are powered on or off. The product reduces forensic backlogs and dedicates resources to collecting evidence. Triage-Examiner does not require an image to be made, but offers that capability. The model tested provides a Lab Add-On, and has three total USBs, which can be used as necessary. Each is clearly labeled and colored differently. This product is easy to use and is mostly automated. There are three steps to complete a scan: install Triage-Examiner, select and define the scan, and analyze the automated reports.

We first installed Triage-Examiner by inserting the Triage Key USB, which required little user interaction, into the target computer. The same key is later prepared to conduct the examination. The first time that the software is implemented requires users to insert the Authentication Key USB to back up the license file. The console opens and users can select either a quick or complete scan. When preparing a scan, the user selects which drive to search and for what to search. From here, the Triage Key can be removed and plugged into any computer. A n auto-run box pops up and the scan can begin. Scans provide a live feed of progress and results by category. Users can suspend the scan at any time to view the results up to the interruption. When the scan is done, evidence is clearly presented in a regimented report, which can be exported as HTML and converted to a PDF. Reports offer tags, which label through color codes evidence by significance. The speed and presentation of Triage-Examiner’s collected evidence was impressive.

The Triage Key has a third functionality, which is replicated in the bootable CD: If a target device is turned off or locked, the USB or CD can reboot the system. The Lab Add-On module one-year software license: $699; one-year license renewal: $499.

The documentation that came with the Triage-Examiner leaves something to be desired. Screen shots are either blurry or small, and there is little to no description per image. Certain instructions are not clearly explicated, though they can be figured out or clarified by customer service – which is not offered 24/7, but is available by phone, email or an online support ticket. The service reps were quite familiar with the product, providing extensive assistance and instruction.

The price for the Triage-Examiner and Lab Add-on, both complete with a one-year license, is $2,187. The one-year license renewal for Triage-Examiner by itself is $999 and is $499 for the Lab Add-on. This product is worth the value. As a forensic examination tool that is used prior to a full investigation, it is very strong.
Cellebrite UFED Ultimate

Cellebrite UFED Ultimate is a forensic tool for gathering information from portable devices, such as cell phones, tablets, PDAs, memory sticks, standalone GPS devices and USB drives. It contains more than 100 different cables to fit almost any phone, GPS or tablet. The system is also capable of supporting more than 7,700 tested devices and regularly updates its list. Additionally, UFED supports more than 3,000 knock-off phones. UFED comes in a heavy-duty carrying case clearly intended for field use. The product can auto-detect a large number of different devices. Once an apparatus is detected, UFED dumps the contents of it onto a USB drive or connected PC. The PC has a reporting application, available at no additional cost, that formats the dumped assets into a useful report.

We received our UFED and after charging the battery the product started right up and offered the choice of selecting a device to test, either manually or by auto-detect. Once a phone or other device is connected and recognized, a cable number is displayed to check whether the correct device and cable are selected. To avoid common user errors and to ensure fast and easy information dumping, UFED provides specific instructions for each device. USB and serial cable types are supported and cables are well-organized to avoid tangling, making it easy to find a specific cable.

Because UFED is used in the field, it is possible that a mobile device will have an uncharged battery, so the product comes with a battery charger-based charger. The testable devices dictate what data is available to UFED. Typically, some older phones and Android devices can cause difficulty. Also, not all mobile devices retain artifacts of deleted data and, therefore, such data may not be recoverable.

We tested several phones with mixed results, which were fully dependent on the device. Smartphones, such as the BlackBerry Bold that we tested, provide a great deal of information. Older phones require that users remove the SIM card and test it separately. The product offers a significant amount of flexibility, but like many forensic tools, we recommend that users become familiar with its strengths to experience its full potential.

UFED excels at providing a quick forensic dump and creating comprehensive reports. The conveniently sized hand-held tool is comfortable to hold and we liked its intuitive user interface. UFED’s real strength as a field kit is its ability to process many mobile devices in a short amount of time. We wish, though, that it had the ability to dump files in an automatic, full forensic investigation. However, we believe the portability, speed and ease of use make it our Best Buy.

Support comes at no additional cost. The website is a work in progress, with a knowledge base planned for the near future. UFED is a bit pricey, but if one is processing large numbers of mobile devices, it will soon pay for itself. The device contains an excellent help menu, allowing users to diagnose problems before contacting support. This product is the easiest-to-use forensic tool for mobile devices we have seen, which translates into efficiency.

Cyber Security Technologies

Mac Marshal Field Edition

Mac Marshal Field Edition from Cyber Security Technologies is a USB tool that allows users to perform a first-level forensic analysis on any Mac or PC computer. It is a small and easy-to-use USB device that comes with licensed software with a unique ID installed directly on the device, so there is no concern about licensing and there is no need to install any other software. Thus, Mac Marshal Field Edition is a plug-and-play USB tool that can be used on many machines without any limitation or additional licensing. In addition to the Field Edition, there are individual software iterations for Mac, PC or both in a single bundle.

The Field Edition that we tested contained both operating environments. When used to examine a live target system, Mac Marshal Field Edition can gather live state information (RAM, running processes, network connections, etc.) that would be lost when seizing the target machine and imaging the disk. Mac Marshal Forensic Edition for Macs runs on a Mac OS X 10.4 or later platform, and Mac Marshal Forensic Edition for PCs runs on a Microsoft Windows XP, or later, platform.

Some of the features that are available on the Forensic edition for Macs are not supported on the Windows iteration. Spotlight searches, for example, are not available for Windows. Spotlight is a metadata indexing system, which is responsible for indexing, acquiring, storing and performing file metadata at the highest level. For indexed files, the Spotlight searching method is quick, with solid performance.

We conducted live testing with this tool on both Mac and PC machines. The procedure is almost the same for both. With a quick review of the manual, users will be able to start employing Mac Marshal in less than five minutes. It uses optimized software that will perform reliably, even on computers that are not high-performance devices. Additionally, the hardware is current, so there are no concerns about compatibility. The functions analyze hard drives, images or partitions regardless of the operating system that is installed on the machine under test.

The documentation provides detailed information about use, access and analysis, making the tool straightforward to deploy. The Forensic Editions require 200 MB disk space for installation. The Field Edition is delivered on a USB 2.0 flash drive and is plugged directly into a live target machine or an investigator’s workstation, thus providing portability for use from one target to another. The target system must be running Mac OS X 10.4 or later (that is, taking an image is not necessary).

Support is included in the price of the product for the first year and, after that, is 20 percent of the product price. Unfortunately, we found the website deficient. We could not find a support section. There is an email support address, but there is no direct support location on the site. That said, there is a section on the site for each product and those sections are quite complete.

Mac Marshal is priced reasonably and we find it a good value.
NIKSUN NetDetector Alpine

NetDetector A/pine v4.2 is the most up-to-date version of NIKSUN’s network traffic-monitoring hardware that audits and informs users of network security threats. NetDetector features include an analysis tool, event viewer and an application reconstruction tool. These are used to analyze how a breach occurred, what data was compromised and by whom, and what can be done to fix the breach. The solution also keeps track of how many times the attack has occurred. The analysis tool allows users to investigate at packet level and analyze network security protocols that are in use. To help prevent malicious attacks, NetDetector allows one to set user-generated rules and choose from NIKSUN edicts regarding IDS signatures.

The event viewer allows users to see logged information, such as the time at which a breach occurred and how serious it was. The application reconstruction tool allows one to rebuild or recover applications, users, images and file transfers. This tool also provides a summary of the applications that were used. The NetDetector application uses an Lb-based web interface. This tool can access information about network traffic and security breaches. This product can then monitor traffic and allow quick access to data found and collected on the network. Data – ranging from immediate records to those several years old – can then be viewed. The more information a user wishes to view, the more time the program needs to load, but the records are still accessible in a timely manner.

Documentation includes step-by-step instructions, complete with screen shots, which definitely contribute to simplifying the setup. A list includes instructions in bold text for the commands, which makes the process easy to follow. And there are several troubleshooting tips, pictures of the icons being used and chapters for each of the special features. There is a user guide accessible through the software, which has a help button for the tools. Each button brings the user to a small description of the apparatus and how it works. The NIKSUN NetDetector A/pine v4.2 A/pine comes standard with a basic, no-cost support plan. NIKSUN also offers standard and premium levels of assistance. Standard includes free upgrades, customer help by telephone, email and return merchandise authorization (RMA). Premium includes free upgrades, customer assistance by telephone, email, online, next-day RMA and hot spares.

The NIKSUN NetDetector v4.2 A/pine comes standard with a basic, no-cost support plan. NIKSUN also offers standard and premium levels of assistance. Standard includes free upgrades, customer help by telephone, email and return merchandise authorization (RMA). Premium includes free upgrades, customer assistance by telephone, email, online, next-day RMA and hot spares. The NIKSUN NetDetector v4.2 A/pine comes standard with a basic, no-cost support plan. NIKSUN also offers standard and premium levels of assistance. Standard includes free upgrades, customer help by telephone, email and return merchandise authorization (RMA). Premium includes free upgrades, customer assistance by telephone, email, online, next-day RMA and hot spares. The NIKSUN NetDetector v4.2 A/pine comes standard with a basic, no-cost support plan. NIKSUN also offers standard and premium levels of assistance. Standard includes free upgrades, customer help by telephone, email and return merchandise authorization (RMA).

PARABEN DEVICE SEIZURE v4.6

Paraben Device Seizure v4.6 is a software package that assists forensic investigators in the examination of mobile devices, allowing data acquisition of both logical and physical devices. The solution is available online for download and offers a demo of the software for up to 30 days or 23 executions. It can be purchased with or without additional hardware, including a power adapter, bag, remote charger, SIM card reader and cables to connect devices. Device Seizure comes with a one-year subscription that includes software updates and delivery of cables for new devices added to the system.

We installed Device Seizure on a personal computer and were able to start the program using the graphical user interface (GUI). We could read an Apple iPhone and iTouch device using the standard Apple USB cable. Within the GUI, it was easy to start a new case and acquire data from a device. Major functions – such as reports, data acquisition, keyboarding and sorting – are located in the top navigation bar, simplifying the process. The devices are grouped on the left, allowing access to individual devices with the option to expand further on a chosen device.

The user manual and update notes provided by the Paraben website list compatible devices and types of information users can extract and report on for each device. During the capture, we noticed that the iPhone (iOS 5.0.1) had to be unlocked to retrieve information. A norther disadvantage is that knowing to system settings by the manufacturer some AT&T and Motorola Android OS devices are unable to be acquired. As well, Apple iOS devices and Google Android devices must be unlocked before Device Seizure can execute.

Once data acquisition completes, it is easy to export the report to a wide variety of formats to view the organized results. We were able to view pictures, sent and received messages, system settings, as well as preferences (including version, if the device was locked or synced to a computer). We especially liked the reporting methods, which allowed PDF, HTML, text and other formats for exporting. The reports could range from an extensive report to a basic text report.

What we found especially interesting was Paraben’s integration with Google Earth, allowing GPS points and routes to be tracked from Maelian and Garmin GPS devices. The ease of mapping data and location points allows more interactive and detailed image of the assets, as well as providing a more thorough report. It is important to note that the type of information gathered depends on the device’s specifications and associated operating system. For example, our scan of a Garmin GPS device (Nuvi 1350) retrieved a route list. Paraben’s website provides access to support, training, and release notes, compatible devices and pricing options. Customer service is available without cost 24/7 and consists of two tiers: basic and new/unsupported devices.

The cost of Paraben Device Seizure ranges from as little as $1,795 to $4,699, and offers the product, hardware, mobile field kits, deployable field kits and forensic bundles (including other Paraben products, such as P2 Commander and Forensic Replicator). Support subsequent to the initial one-year subscription costs $360 per year.
**RSA NetWitness**

RSA NetWitness is a network-monitoring system designed to handle a wide range of information. NetWitness comes in three parts: a Concentrator (a Linux-based network appliance), Decoder (a configurable network-recording appliance) and Investigator (an interactive threat analysis application). All three elements are critical to ensure that the product is working properly. Initially, we only had the Concentrator and Decoder activated. The Investigator was lost in the mail. Upon receiving all portions of NetWitness, and getting them to work together, we were finally able to dive into the product.

NetWitness proved to be a difficult product to set up. The installation directions for the software and hardware are minimal, which resulted in our making several mistakes during system configuration. Too, it was difficult to obtain solutions since we received the incorrect key for different clock times between the NetWitness investigator and decoder.

But, once the product was up and running, we found the tool to be compelling. Not only did it capture every packet traveling through the network, but it organized the report in a way that users can quickly reference. Certain functions allow users to implement the packets for risk assessment by way of analyzing all traffic on the network. Furthermore, packets capture is not restricted to LANs, but extends to wireless traffic. The Decoder and Concentrator took some time to grow familiar with, but eventually became fairly easy to navigate. The tool tips were helpful in navigating our way through the application. The investigator was another matter, however. It was slightly confusing to navigate, and the amount of information it provided was overwhelming on occasion. But, after getting used to the immense reports, this tool began to shine.

User documentation, excluding the installation directions, was helpful, presenting solid instructions. The user guide was straightforward and attempted to walk the admin through most of the process, but some sections left us in the dark for certain functions.

Too, the support for RSA NetWitness is spotty. When users navigate through the company’s automated phone system, they are placed on hold for quite some time until tech support makes contact. When this happened with us, the service representatives were very accommodating. Not only were they patient with our own network issues, but they eventually became fairly easy to navigate. The tool tips were helpful in navigating our way through the application. The investigator was another matter, however. It was slightly confusing to navigate, and the amount of information it provided was overwhelming on occasion. But, after getting used to the immense reports, this tool began to shine.

User documentation, excluding the installation directions, was helpful, presenting solid instructions. The user guide was straightforward and attempted to walk the admin through most of the process, but some sections left us in the dark for certain functions.

The common thread for all past ProDiscover IR reviews in SC Magazine has been ease of use and flexibility, and this review is no exception. From installation to testing, we experienced few problems. The software was easy to use and the graphical user interface (GUI) was easy to navigate. With a basic understanding of forensics, one can accomplish many things with this tool. For testing, we followed all instructions in the provided manual – even though many were no-brainers owing to the intuitive nature of the GUI. ProDiscover IR was able to image and preview all advertised file systems without issue, either fixed or remote. “Stealth mode” held true to its name as the agent was installed undetected in the target system’s directory without visibility on the program bar or tray area. We also enjoyed the customizable report generator, which further added to the efficiency of this program.

The only instance where we encountered a challenge was during analysis. We experienced multiple freezes and crashes when navigating around the project tree, all of which were properly documented in crash dump files. These could have been related to the size of the memory on our test computer. In the case of our test machines, we were running Windows XP in a 32-bit configuration. ProDiscover’s ProScript highlighted this software’s true potential. The ProScript Perl engine changed to Strawberry Perl in v7.1.0.0, which made it easier to use on Windows machines through the MiniW (Minimalistic GNU for Windows). Technology Pathways provides basic tutorials for ProScript, which helpfully supplements and supports users who may not be so familiar with Perl. All in all, we found its operations ran parallel to its advertised functionality, albeit it was a little touchy with crashes.

Documentation that came with this product was satisfactory. Everything was easy to read and understand. The section headers and content were logically placed, direct and helpful. Support has not changed markedly from past reviews; no-cost 30-day warranty with an optional fee-based “annual software maintenance” (including software updates and telephone/email assistance) at $1,619.10. Aside from this option, the website provides an extensive knowledge base, complete with advanced tips and essential ProScript code snippets. Given the flexibility, utility and range of tools, $8,995 is reasonable for any mid- to large-sized company.
WetStone Technologies US-LATT

On our first encounter with WetStone Technologies US-LATT, we studied the various manuals and articles, as well as the WetStone website, to gain an understanding of the text and product. US-LATT is a live acquisition and triage tool generally used by law enforcement to quickly investigate suspect computers, providing these agencies and first responders the ability to analyze multiple systems at one time. This system is generally cooperative, but we did find one thing aggravating: the configuration utility was difficult to deploy. The utility proved a struggle to download and install, requiring us to place the installer on a disc for easier access. Once the utility was installed, we still encountered a series of error messages, giving the impression that the program was not fully compatible with the system. This is not something an onsite investigator wants to see when performing data acquisition. A filter ignoring the error messages, the utility seemed to work well. Once the kinks are worked out in initial setup, the equipment performs adequately, working according to the defined parameters. Actual data acquisition time was not very long and results were quickly presented. This is where US-LATT showed its prowess, regardless of its simplistic design. A nd, its portability gives investigators the ability to analyze multiple systems at one time. This is an especially welcome feature when investigating large companies whose networks include many suspect computers. However, the product has some problems with compatibility on varying systems, as well as a limited list of compatible devices. For example, US-LATT relies on the fact that most suspects will have recent versions of Windows operating systems.

The offering features a one-year maintenance package with 24-hour support. Customer assistance is also available by email. Documentation is easy to follow. The manual is in PDF form and certain terms can be searched for, which allows quick referencing. Plus, the digital manual feature means that it can be accessed on any device with the storage or connectivity for access. One negative is that the system utility allows for a quick erase of imported data. This is convenient for easy removing information, but without access controls, that feature might pose integrity and availability issues.

WetStone Technologies do it under contract with the National Institute of Justice, which provides US-LATT free for state and local law enforcement. Otherwise, the basic price is $1,495, with free one-year product maintenance included in the initial purchase. Beyond that first year, renewal is $299. The website also offers online training for $500. We recommend this product because it is ideal for field use, despite some complications.

AccessData Group Forensic Toolkit (FTK) v4

The suite of computer forensic tools from AccessData Group that we tested is a nearly complete examiner’s tool kit. Add its Password Recovery Toolkit, not reviewed here and you’ve got the whole shebang. The new FTK 4 is pretty much the same set of tools that we are used to seeing from AccessData – until you add the company’s exciting new modules, Cerberus and Visualization. Now, it’s a whole different ballgame.

These two new modules allow examiners to perform a deep dive into malware on the disk under examination (Cerberus) and to examine email and documents in an entirely new way (Visualizer). The Mobile Phone Examiner Plus (MPE+) adds mobile devices to the repertoire. It outputs a file that can be added directly into a case, along with images from computers. This makes correlation fast and straightforward.

We read two hard-disk images into FTK 4 and then added dumps from two mobile devices. All of these images were placed into a single case which was then processed. We found the performance to be exceptional and the results of having all of the images – computers and phones – in the same case made analysis easy.

The new modules are quite impressive. There is a clear graphical display of the relationships between email addresses using Visualizer. Similar visualization enhancements are available for document files. Using the Visualizer is easy and we had no trouble performing the additional analysis that the tool permits.

Today, malware in its many forms bedevils security engineers and forensic examiners alike. It is always challenging to identify malware – especially zero-day – using conventional computer forensics. Cerberus changes that. We ran the post-processing necessary to do a Cerberus analysis. With that, every time we opened a file that could contain malware, we received the Cerberus report for that file. The report gives deep details about the file and adds a probability that the file is or contains malware.

MPE+ was provided to us in a Microsoft tablet, but it is also available as software only. The product is the same in either case. The kit we received has a solid collection of cables. We were able to connect our phones and dump them in under 30 minutes each. The time this takes depends, of course, on the size of the data in the mobile device. One can read a standalone report from MPE+ or generate a file that can be added into an FTK analysis. We did both and concluded that this tool’s biggest strength is its ability to act in concert with the overall investigation.

Pricing for this suite of tools is competitive in the computer forensic market, in general, but the breadth and depth covered makes it an excellent value. FTK and the rest of its complementary tools do not take long to learn. They cover a lot of forensic ground and, having used them in actual cases as well in the test lab, we can say that they provide a solid, reliable platform and consistent look and feel.

Documentation, in the form of PDF files, is excellent. The AccessData Group website is complete and provides the support needed.
Mitigating the next WikiLeaks

The operating environment itself must be altered, says Dan Geer.

WikiLeaks as poetry? With lines like, “If neither foes nor loving friends can hurt you...” Rudyard Kipling’s bracing poem “If,” challenges the reader to face uncertainties, including the uncertainty of never knowing from where a threat can come. WikiLeaks does the same, with one exception: It exemplifies the reader to face uncertainties, including the uncertainty of never knowing from where a threat can come. WikiLeaks does the same, with one exception: It exemplifies the

...authorization systems are not deterrents to the insider threat.”

In this fully connected world, a growing body of civil law demands the public shaming of any corporation that leaks other people’s data. Financial regulations already in place are beginning to treat data leakage events as inherently material, thereby elevating such matters to the boardroom level. Furthermore, designers of national policy are proposing to make protection against insider attacks a mandate that includes a periodic inspection regime.

To be an insider, the individual must already have passed through an access control gate. That’s what takes them “inside,” of course. Therefore, access control is not, and never can be, a deterrent to the problem of the insider threat. An insider perpetrator, to do his or her job, must have authorization credentials congruent with the task they must do. So, they are either trusted individuals or have discovered a way in. In either case, authorization systems are not deterrents to the insider threat, though they may bound the downside consequence, to a degree.

Some members of staff must have special authority simply because keeping the IT plant running requires interventions that cannot be anticipated, such as when parts fail. Such special authorities may also be available to any internal investigations team that may be in place, and similarly to any internal “red team.” It is not necessarily bad – but it is a reality – that there will always be people in positions who are capable of being an insider threat. The question is how to control this by some means that is not itself subject to the very legitimate capabilities of the determined and knowledgeable insider.

The answer is that the operating environment itself must be altered. Of all possible design goals for any security system, perhaps the most important, the one with the highest value, is “No silent failure.” If we must alter the operating environment in a manner consistent with preventing the invisible or silent failure of an expert insider attack, the engineering problem is at least well specified.

The most cost-effective solution to this engineering problem is to instrument the operating environment so that data does not move without that movement being observed by the instrumentation. The transition from data-at-rest to data-in-motion always involves the operating environment, and does so in a way that is directly subject to instrumentation. That the instrumentation is difficult to do without side effects is a given. That the instrumentation – the event-detection mechanism – is in place can serve as a deterrent to the insider threat.

Only when this type of mechanism is in place can enterprises focus on another enterprise artifact: the human behavioral issues and their policies governing data handling. Technology alone, and human oversight alone, cannot solve the problem.

Dan Geer is a well-known computer security analyst and chief scientist emeritus at Verdasys, a Waltham, Mass.-based provider of enterprise information protection solutions.

The answer is that the operating environment itself must be altered. Of all possible design goals for any security system, perhaps the most important, the one with the highest value, is “No silent failure.” If we must alter the operating environment in a manner consistent with preventing the invisible or silent failure of an expert insider attack, the engineering problem is at least well specified.

The most cost-effective solution to this engineering problem is to instrument the operating environment so that data does not move without that movement being observed by the instrumentation. The transition from data-at-rest to data-in-motion always involves the operating environment, and does so in a way that is directly subject to instrumentation. That the instrumentation is difficult to do without side effects is a given. That the instrumentation – the event-detection mechanism – is in place can serve as a deterrent to the insider threat.

Only when this type of mechanism is in place can enterprises focus on another enterprise artifact: the human behavioral issues and their policies governing data handling. Technology alone, and human oversight alone, cannot solve the problem.

Dan Geer is a well-known computer security analyst and chief scientist emeritus at Verdasys, a Waltham, Mass.-based provider of enterprise information protection solutions.

In this fully connected world, a growing body of civil law demands the public shaming of any corporation that leaks other people’s data. Financial regulations already in place are beginning to treat data leakage events as inherently material, thereby elevating such matters to the boardroom level. Furthermore, designers of national policy are proposing to make protection against insider attacks a mandate that includes a periodic inspection regime.

To be an insider, the individual must already have passed through an access control gate. That’s what takes them “inside,” of course. Therefore, access control is not, and never can be, a deterrent to the problem of the insider threat. An insider perpetrator, to do his or her job, must have authorization credentials congruent with the task they must do. So, they are either trusted individuals or have discovered a way in. In either case, authorization systems are not deterrents to the insider threat, though they may bound the downside consequence, to a degree.

Some members of staff must have special authority simply because keeping the IT plant running requires interventions that cannot be anticipated, such as when parts fail. Such special authorities may also be available to any internal investigations team that may be in place, and similarly to any internal “red team.” It is not necessarily bad – but it is a reality – that there will always be people in positions who are capable of being an insider threat. The question is how to control this by some means that is not itself subject to the very legitimate capabilities of the determined and knowledgeable insider.

The answer is that the operating environment itself must be altered. Of all possible design goals for any security system, perhaps the most important, the one with the highest value, is “No silent failure.” If we must alter the operating environment in a manner consistent with preventing the invisible or silent failure of an expert insider attack, the engineering problem is at least well specified.

The most cost-effective solution to this engineering problem is to instrument the operating environment so that data does not move without that movement being observed by the instrumentation. The transition from data-at-rest to data-in-motion always involves the operating environment, and does so in a way that is directly subject to instrumentation. That the instrumentation is difficult to do without side effects is a given. That the instrumentation – the event-detection mechanism – is in place can serve as a deterrent to the insider threat.

Only when this type of mechanism is in place can enterprises focus on another enterprise artifact: the human behavioral issues and their policies governing data handling. Technology alone, and human oversight alone, cannot solve the problem.

Dan Geer is a well-known computer security analyst and chief scientist emeritus at Verdasys, a Waltham, Mass.-based provider of enterprise information protection solutions.
Thank you!

SC Magazine readers choose ESET No.1
Best Anti-Malware Management

And the best keeps getting better—
IT experts everywhere agree.