Malware is increasingly finding ripe new territory on the mobile platform. P16

The agency that stepped up
The FTC has become the de facto enforcer of data privacy laws and regulations. P21

Closing the gate
Even when you’ve got an insider gone bad, there are ways to limit the damage and protect data. P24
REGULARS

4 Editorial: Is this an evolution or a devolution?

6 Threat report: A Russian amased 20 million email addresses.

8 Threat stats: A Morgan Stanley employee stole client information.

10 Update: Journalist Barrett Brown was sentenced to 63 months in prison.

11 Debate: The financial industry is better at cybersecurity than other industries.

12 Two minutes on...: Challenges of a splintered market.

13 Skills in demand: Application security engineers are needed.

14 From the CSO’s desk: Targeted attacks: Are you prepared?, Zouhair Guelzim, CISO, L’Oréal Americas.

15 Last word: Communicating security concepts, by Scott Aurnou, vice president, SOHO Solutions.

FEATURES

16 Malware on the move: Like virtually all online threats, malware is increasingly finding a ripe new territory on the mobile platform, says Justin Somaini, chief trust officer at Box.

21 The agency that stepped up: The FTC has become the de facto enforcer of data privacy laws and regulations.

24 Closing the gate: Data leak prevention: Even when you’ve got a breach or an insider gone bad, there are still ways to limit the damage and protect data.

28 The whole package: Security certs: Security certifications can land you a better job, but companies are also looking for people who can communicate and manage projects.

PRODUCT REVIEWS

33 Product section: The evolving trend in vulnerability management is to test constantly and remediate as you go.

34 Group Test: Vulnerability management: When we want to manage vulnerabilities we are, in a sense, managing risk. To do that we need to understand what vulnerabilities are in the enterprise.

Is this an evolution or a devolution?

A t the start of this year, I was talking to a CEO buddy of mine who was trying to squash any impending issues that might have seemed to be rising in data breaches. He voiced his expectations that because of the Sony compromise and many other high-profile security posture attacks that took place last year, organizations were going to be spending more money on security.

The interesting thing, though, is that when I asked him just how much he was upping the coffers for IT security-related expenditures in his own company, he faltered. You see, although he was much more aware of the ever-increasing possibilities of his company becoming victimized by cybercriminals, the budgeters tied specifically to security projects he approved for the year were flat.

It’s not the only CEO who, while acknowledging how crucial a role information security is now to an organization’s longevity and success, also puts off spending more on it. Security investments still frequently get delayed by CEOs and their boards. The thinking still seems to be that if the basics are in place and more of these conversations and they all seem to convey the same thing — that leaders like my CEO pal expect the company’s IT security posture to be staunch enough to thwart attackers. They surely don’t want to be the next Sony, the next Anthem. Yet, they also have some serious trouble actually making not just seeing — IT security as a major keystone of business operations.

So we’re still witnessing nimble and crafty CISOs getting creative and looking at IT security implementations to see where automation and other means of streamlining information assurance practices can be done. Many of these savvy CISOs also are working more closely with business units than ever before, trying to ensure that IT security costs are built into their individual projects from the jump.

The hope is that we’ll see security becoming more the responsibility of the entire organization. So, CEOs may not just be talking about security over a beer with someone like me, but will be having more fruitful and more beneficial discussions with the pros charged with safeguarding their corporate infrastructures and the data on them.

Iline Armstrong is VP, editorial of SC Magazine.
Germany top producer of zombie IP addresses
For the period reported, the EMEA region (Europe, Middle East, Africa) was the leading source of all zombie IP addresses. Of the countries making up the EMEA, Germany was the top producing country. For the other regions, the top producers were Argentina in South America, the U.S. in North America and China in the Asia-Pacific region. Source: Symantec

Cyber criminal activity across the globe, plus a roundup of security-related news

**CANADA** – Citing documents leaked by whistleblower Edward Snowden, reports indicate that the Communications Security Establishment – Canada’s version of the NSA – has a program designed to track millions of downloads and uploads. The project, known as “Levitation,” enables analysts to access information on roughly 15 million uploads and downloads from free websites each day.

**CANADA** – SentinelOne researchers reported that a new variant of the Zeus trojan is targeting a number of banks in Canada, including Bank of Montreal, Royal Bank of Canada and National Bank of Canada. The variant is spreading via social engineering and exploit kits.

**NETHERLANDS** – A Dutch judge approved the extradition of Vladimir Drinkman, a Russian man who was arrested in June 2012 in the Netherlands. Drinkman is charged with hacking payment companies, most notably Heartland Payment Systems. He will be extradited to New Jersey.

**RUSSIA** – An attacker exploited a vulnerability and amassed 20 million email addresses belonging to users of dating website Topface. The attacker put the email addresses up for sale online, but Topface tracked the individual down and offered an award for finding a vulnerability. The company said the attacker would not distribute the data.

**CANADA** – SentinelOne researchers reported that a new variant of the Zeus trojan is targeting a number of banks in Canada, including Bank of Montreal, Royal Bank of Canada and National Bank of Canada. The variant is spreading via social engineering and exploit kits.

**SUMMIT, N.J.** – New York Jets linebacker Jermaine Cunningham was arrested and charged with violating New Jersey’s revenge porn law, as well as with other counts. Cunningham was arrested after police responded to a domestic dispute at his home. He faces one count each of third-degree privacy violation and criminal mischief, as well as a fourth degree unlawful weapon transfer charge.

**BARTLETT, Ill.** – Two 16-year-old Bartlett High School students face felony charges after authorities alleged that the males hacked into their school’s computer system and changed attendance records, as well as accessed the email account of at least one district staff member. One student was charged with aggravating computer tampering and the other student was charged with computer fraud.

**AUSTRALIA** – Information from a large-scale data breach, which in December impacted Australian travel insurance company Aussie Travel Cover, was leaked online. A report claimed an Australia-based hacker stole troves of data from two of the company’s databases, which contained a total of more than 870,000 personal records. The data included names and home addresses, as well as partial credit card numbers.

**TEL AVIV, ISRAEL** – An alleged attacker who hacked the computers of multiple international artists, including Madonna, was arrested in Tel Aviv. Israel’s version of the FBI, Lahav 433, nabbed the 39-year-old suspect after an Israeli firm made a breakthrough in the case and gave its findings to the police.

Colored dots on the map show levels of spam delivered via compromised computers (spam zombies). Activity is based on the frequency with which spam messaging corresponding with IP addresses is received by Symantec's network of two million probes with a statistical reach of more than 300 million mailboxes worldwide.
There were 2.9 million attacks in the U.S. last month.

Top 10 names used by phishing websites

1. Facebook 5,533,422
2. mail.com 4,896,748
3. Google 3,223,481
4. LinkedIn 1,967,287
5. ticketmaster 1,383,116
6. Microsoft 1,327,978
7. @MAIL.RU: 1,291,720
8. CNBC 1,283,209
9. American Express 1,113,322
10. EarthLink 993,487

Top breaches in January

Name | Type of breach | Number of records
--- | --- | ---
Morgan Stanley | A Morgan Stanley employee stole client information including account numbers. | 350,000
Mount Pleasant School District | Present and former staff members were informed that their personal information may have been compromised between Jan. 18 and 21. | 915

TOTAL number of records containing sensitive personal information involved in breaches in the U.S. since January 2005: 1,012,730,026 (as of Feb. 12)

Top 5 sources of spam

United States 19.18%
Ukraine 15.15%
China 6.18%
Russian Federation 5.78%
France 5.35%

Top 5 attacked countries

Croatia 2.06%
Kazakhstan 1.55%
Ukraine 1.54%
Bulgaria 1.54%
Algeria 1.53%

Top 5 business apps used by phishing websites

1. Facebook
2. mail.com
3. Google
4. LinkedIn
5. Ticketmaster

Top 5 threats

1. Ramnit.I
2. Ogimant.genic
3. Elkem.B
4. Picys.C
5. Tudpay.A
6. Lmit.AAV
7. Soltrn.L
8. Ramnit.J
9. Gupboot.B
10. Laring

Index of cyber security

<table>
<thead>
<tr>
<th>Index value</th>
<th>Rate of change (continuously compounded)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.550</td>
<td>1.50</td>
</tr>
<tr>
<td>2.500</td>
<td>1.40</td>
</tr>
<tr>
<td>2.450</td>
<td>1.30</td>
</tr>
<tr>
<td>2.400</td>
<td>1.20</td>
</tr>
<tr>
<td>2.350</td>
<td>1.10</td>
</tr>
<tr>
<td>2.300</td>
<td>1.00</td>
</tr>
<tr>
<td>2.250</td>
<td>0.90</td>
</tr>
<tr>
<td>2.200</td>
<td>0.80</td>
</tr>
<tr>
<td>2.150</td>
<td>0.70</td>
</tr>
<tr>
<td>2.100</td>
<td>0.60</td>
</tr>
<tr>
<td>2.050</td>
<td>0.50</td>
</tr>
<tr>
<td>2.000</td>
<td>0.40</td>
</tr>
<tr>
<td>1.950</td>
<td>0.30</td>
</tr>
<tr>
<td>1.900</td>
<td>0.20</td>
</tr>
<tr>
<td>1.850</td>
<td>0.10</td>
</tr>
<tr>
<td>1.800</td>
<td>0.00</td>
</tr>
<tr>
<td>1.750</td>
<td>-0.10</td>
</tr>
<tr>
<td>1.700</td>
<td>-0.20</td>
</tr>
<tr>
<td>1.650</td>
<td>-0.30</td>
</tr>
<tr>
<td>1.600</td>
<td>-0.40</td>
</tr>
<tr>
<td>1.550</td>
<td>-0.50</td>
</tr>
<tr>
<td>1.500</td>
<td>-0.60</td>
</tr>
<tr>
<td>1.450</td>
<td>-0.70</td>
</tr>
</tbody>
</table>

The index queries information security industry professionals monthly to gauge their perceived risk to the corporate, industrial and governmental information infrastructure from a spectrum of cyber security threats. A higher index value indicates a perception of increasing risk, while a lower index value indicates the opposite.

Source: ICS, www.cybersecurityindex.com

Top 5 attacks used by U.S. hackers

1. Upatre downloader trojan
2. Rerdom trojan
3. Pushdo trojan
4. Ahtymaim trojan
5. Waledac trojan

Top 5 attacks used by foreign hackers

1. ZeroAccess trojan
2. Butterfly bot
3. Gozi trojan
4. Waledac trojan
5. Nymaim trojan

Source: Dell SecureWorks

Source: CYREN (formerly Commtouch Software Online Labs)

Source: DataLossDB.org, hosted by the Open Security Foundation

Source: Kaspersky

Source: ICS, www.cybersecurityindex.com

Source: Motive Security Labs

Source: Kaspersky

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

Source: SCMagazine.com

Source: Dell SecureWorks
Researchers at Qualys discovered a buffer overflow vulnerability in the Linux GNU C Library (glibc) that, if exploited, could enable an attacker to remotely take complete control of a victim’s system — all without having knowledge of system credentials. The high severity bug, CVE-2015-0235, was named GHOST because it can be triggered by the ‘GetHOST’ functions, Qualys noted. Debian 7 (Wheezy), Red Hat Enterprise Linux 6 and 7, CentOS 6 and 7, and Ubuntu 12.04 are among the systems that are affected, and other Linux systems using versions of glibc from 2.2 to before 2.18 are also at risk. Researchers said that the best way to protect against GHOST is to apply available patches from Linux distribution vendors.

On the heels of President Obama’s call for federal data breach legislation, a senator announced that he was penning a bill that carried a 30-day notification requirement for breached entities. The requirement, which Obama also proposed in a January speech at the Federal Trade Commission (FTC), would supplant state data security and breach notification laws, Sen. Bill Nelson, D-Fla., revealed in a draft summary of the bill. Under the legislation would authorize the FTC and state attorneys general “to enforce the data security and breach notification provisions of the Act,” meaning that entities could face civil penalties levied by the FTC ever “unfair or deceptive acts or practices under Section 18 of the FTC Act,” the draft summary said.

The White House’s proposed revisions to the Computer Fraud and Abuse Act (CFAA) raised alarm in the IT security community which continues to await amendments to the federal anti-hacking law, long criticized for being out-dated and leading to the aggressive prosecution of those in the field. Major contention arose from one revision, in particular, which would raise penalties for circumventing digital access barriers from starting to misdialing a message. Other security pros, such as Katie Moussouris, chief policy officer at HackerOne, expressed concern about the “expanded language” of the legislative proposal, which could hamper vulnerability research and security testing activities, and perhaps, even breach reporting. She noted that CFAA, the law under which Aaron Swartz was pursued before his suicide two years ago, has always intimidated researchers.

Debate The financial industry really is better at cybersecurity than other industries.

In spite of some of the breaches recently reported, the financial sector, particularly in the United States, remains one of the best in terms of cybersecurity — not necessarily because it’s doing everything right, but because everyone else is doing it so terribly wrong. Most of all, the big banks have done a better job than other industries of prioritizing cybersecurity. We see this in their annual budgets, which actually earmark a significant portion to network defense (from security executives to third-party pen-tests, etc.). We also see it in their investments in the cloud and fraud detection. They’ve done this because they have to — banks live or die by their image. So for them, it’s not just about protecting their data, it’s almost equally about protecting their reputations too.

The financial industry has really led the way in a number of areas, including intra-industry coordination (FS-ISAC and Soltra Edge are two great examples), anomaly detection, the cloud, exfiltration filters and firewalls.

For a long time, the assumption has been that major financial institutions are the “crème de la crème” of the IT security world. But is this really true? Recent disclosures by JP Morgan, Nasdaq and even the string of DDOS attacks on banks starting in 2012 should cast doubt on this assertion. It is true that banks spend more money on IT security than most other organizations, and that’s commendable, but it doesn’t mean those expenditures translate into top-notch security. Instead, they’re buying all the latest tools the market can offer while not managing security incident response properly. Financial institutions remain plagued by a number of key security problems, such as long procurement phases, a fear of change that’s deeply ingrained within the management structure, not enough cyber decision-makers who can make the tough calls on IT security, a reliance on outdated methods of email/ticket/manual management systems, little or few frameworks or controls in place around incident response, simulations and training, etc.

The SC Magazine Poll
Do you believe President Obama’s recent comments regarding cybersecurity will hasten national data breach legislation?

The Stats
47 state breach notification laws (plus District of Columbia, Guam, the Virgin Islands and Puerto Rico).

90% of the 500 data breaches in the first half of 2014 were avoidable.

For

AGAINST

Against

![Dave Aitel, CEO, Red Team Research](http://www.scmagazine.com)

![Hans Zenck, CEO, CyberSponse](http://www.scmagazine.com)

![Aaron Swartz](http://www.scmagazine.com)

* Championing a free and open internet, Swartz changed the way we consume information. His pursuits had the result of a strike at the heart of the U.S. government, bringing him a three-year prison term. Shortly after his death in January 2013, a judge reduced his sentence to 63 months in prison, minus time served to 6 months in prison, minus time served to 6 months in prison, minus time served to 6 months in prison.*

* Swartz was pursued before his suicide two years ago, has always intimidated researchers.

* Sen. Bill Nelson, D-Fla., revealed in a draft summary of the bill. Under the legislation would authorize the FTC and state attorneys general “to enforce the data security and breach notification provisions of the Act,” meaning that entities could face civil penalties levied by the FTC ever “unfair or deceptive acts or practices under Section 18 of the FTC Act,” the draft summary said.

* The White House’s proposed revisions to the Computer Fraud and Abuse Act (CFAA) raised alarm in the IT security community which continues to await amendments to the federal anti-hacking law, long criticized for being out-dated and leading to the aggressive prosecution of those in the field. Major contention arose from one revision, in particular, which would raise penalties for circumventing digital access barriers from starting to misdialing a message. Other security pros, such as Katie Moussouris, chief policy officer at HackerOne, expressed concern about the “expanded language” of the legislative proposal, which could hamper vulnerability research and security testing activities, and perhaps, even breach reporting. She noted that CFAA, the law under which Aaron Swartz was pursued before his suicide two years ago, has always intimidated researchers.

* The financial industry has really led the way in a number of areas, including intra-industry coordination (FS-ISAC and Soltra Edge are two great examples), anomaly detection, the cloud, exfiltration filters and firewalls.

* The financial industry really is better at cybersecurity than other industries.
Challenges of a splintered market

In new budgets, both at organizations and the government, one thing’s for sure: Cybersecurity spending continues to trend upward. According to Gartner, IT security spending surpassed the $70 million mark in 2014, a 7.9 percent increase from 2013. The firm also predicted this trend to continue into 2015, ultimately reaching the $76.9 million mark.

A looming federal data breach notification law coupled with the president’s budget proposal for the 2016 fiscal year – featuring a $14 billion allotment toward government cybersecurity efforts – signals a high demand for solutions. If one adds the headline-grabbing breaches that continue to crop up, organizations are pressed to arm themselves for the inevitable breach.

But with a slew of vendors in the market offering an array of solutions, how easy could it be for security professionals to choose where to allocate their budgeted cybersecurity spend? Trade shows like the RSA Conference and InfoSecurity Expo have floors showcasing veteran and start-up security firms, an intimidating scene for attendees looking for new tools. Alex van Someren, managing partner at Ama-

derator, believes the market’s fragmentation poses a serious problem for end-users who are struggling to find comprehensive solutions from a single vendor.

“The user-experience is damaged by the need to integrate multiple products, which usually doesn’t go well from a user-experience point of view,” van Someren says, adding that finding the best possible solution is “pretty hard work.”

Like van Someren, Peter Stephenson, CSIO at Norwich University (and SC Magazine’s technology editor heading up the product reviews), believes that the mentality of many start-ups harkens back to a 1990s’ mentality. “I’m going to build the next great thing – or, maybe just some thing, great or not – in my garage, sell it to Google and roll in money,” he says. The good news, he points out, is that there are newbies offering innovative and unprecedented solutions.

“I absolutely revel in finding a smart, small startup where the founders have really identified a serious problem and have come up with a creative solution to the problem that can be used easily by customers,” Stephenson says.

The intersection between improving the user experience and delivering high security are what many of these up-and-coming vendors may need to aim for. — Marcus Colón

$76.9M projected investment in cybersecurity in 2015.

Source: Gartner

JOBS MARKET

Me and my job

Bob West

chief trust officer, CipherCloud

How do you describe your job?

A good portion of my role is acting as an advocate for my company’s customers and providing them with guidance throughout their cloud journey. I help customers understand the lay of the cloud information-security land. Then, based on an analysis of their IT ecosystem, I help them assess the best solutions and practices for overcoming the security, privacy and residency risks that they face. It’s easy for me to provide them with the proper guidance given my prior experience in the corporate world.

What keeps you up at night?

Thinking about how much intellectual property is being stolen from private sector companies.

Why did you get into IT security?

I was looking to make a transition from Citicorp (now Citigroup) in 1994 and interviewed with Ernst & Young for a role in a nascent information-security consulting practice. It seemed very interesting to me and my background in operating systems and networks was a good foundation to learn more about security. I had the opportunity to work with some of the best people in the firm and that was a great beginning to the rest of my security career.

What was one of your biggest challenges?

Learning that the business drives everything and security needs to be aligned with both business and technology strategy.

What makes you most proud?

I’ve had the opportunity to have a significant impact on a large number of companies through both my bank and the security startups in which I’ve been involved.

How would you use a magic IT security wand?

I would give all technologies and security professionals great communication and business skills.

Skills in demand

The need for application security engineers has grown as legacy applications are moved to the web. The position can be focused on enterprise or mobile applications, but the overall goal is similar: consider all system vulnerabilities of applications from design/development through implementation and maintenance.

What it takes

Hands on experience with secure code review, static analysis/security testing, dynamic application security testing and strong knowledge of web development technologies.

Compensation

Base compensation can range from $100K-$175K, often with additional incentives.

—Donna Clark, principal, Baccharelli Consulting and founder of www.bizjetCounsel.com

Briefs

Company news

Gerald Choung has joined San Diego-based ESET, a security software company, as vice president of sales. Choung will lead the North American sales team and provide strategic direction for ESET’s partner and distributor network. Choung worked at a variety of Fortune 500 companies before joining ESET, most recently as senior director of channel strategy and sales for Qualcomm. ESET claims more than 100 million users and employs more than 200 people at its North American headquarters.

Mary Landesman has joined San Francisco-based Norse, a live attack intelligence firm, as senior data scientist. Landesman will help the company detect and analyze cyber threats and also develop prevention tactics. She has worked in the industry for more than two decades, most recently at Cisco Systems as a senior security researcher. While there, she analyzed data sets to determine the most recent web-based security trends.

San Francisco-based secure mobile gateway pioneer Wandera announced $25 million in additional funding. This latest funding was led by 83North, with participation from existing investor Bessemer Venture Partners. This brings Wandera’s total funding to $23 million.

William Welch has joined San Jose, Calif.-based Zscaler, an internet security company, as global vice president of sales and chief revenue officer. Welch will scale Zscaler’s sales and channel organizations and help accelerate the company’s global growth. For more than 25 years, Welch served in executive sales roles at public technology companies. He was most recently the vice president and GM for HP Software Americas, where he was responsible for more than $2 billion in sales.

William Welch, global VP of sales and chief revenue officer, Zscaler

Bastille, an Atlanta-based Internet of Things (IoT) threat detection and mitigation provider, has extended its angel round with a $1 million investment. Funding comes from David Cowan of Bessemer Venture Partners. This is the second time Cowan has backed Bastille’s founder Chris Rouland. The extended angel round will allow Bastille to continue engineering and support pilot programs.

Secure Islands, an Israel-based advanced information protection and control (IPC) solutions provider, has opened its North American headquarters in New York and appointed Paul Gabrik as the executive vice president of sales. Gabrik will develop and manage the company’s sales strategies for enterprise customers in the Americas. Previously, Gabrik served as the global sales lead executive managing partner at Accenture Software Practice.

Follow us on Facebook, LinkedIn and Twitter.
Targeted attacks: Are you prepared?

Zouhair Guelzim
VP and CISO, L’Oréal Americas

Without a doubt, hackers are becoming more sophisticated, well-organized and mission-driven. They are increasingly using advanced persistent threats (APTs) methods and every tool at their disposal. Hackers are finding new attack vectors to exploit and it is becoming harder for us “security professionals” to defend our organizations. APTs are targeted, well-organized attacks, often aimed at an organization’s most valuable assets. Because of the skillfulness of these smart attackers, APTs are more difficult to detect and prevent than traditional security threats. These advanced threats require the information security function to rethink its approach to operations.

The pressure is on! Is your organization prepared? Many enterprises have not kept pace and lack the necessary fundamentals required to prepare and plan against simple cyber attacks, let alone advanced and targeted attacks. To prepare, keep these priorities in mind:

First, build your organization’s intelligence capabilities. This will allow you to get a better perspective of threats, think “Big Data.” Most organizations recognize the need to improve analytics to combat APTs. However, many analytic programs fail because they collect vast amounts of data without a clear sense of how the data will be analyzed to produce actionable information, let alone having the adequate amount of resources to review the data.

Second, revamp your security controls. Most controls focus on conventional threats, making them less suited to defend against today’s inculpations. Rather, you should align controls to a threat-based framework, such as the kill chain. This will allow you to easily conduct gap analysis on advanced threats and build your defense lines.

Third, develop a better approach to manage threats. This requires the information security organization to change focus from known vulnerabilities to understanding high-targeted threats. With this transition, you must integrate a new set of activities into gathering intelligence, conducting threat analysis to identify threats and disseminating information to prevent future attacks.

A practical approach to intelligence gathering is identifying evidence of a recent attack in existing logs or identifying what kind of logs would record an element of a known attack. Then, expand ways to detect it by identifying what other tools or resources could have detected the attack. Once you have identified the tools, try applying the process to other threats by using an informed approach to collect data and design search queries. The results will produce quick wins that will support further investments and allow time for staff to build expertise.

What’s your strategy for defending your data?

W

How far have we come?

I

Identity management has evolved rapidly over the past decade and persistent demand for identity assurance means that more change is inevitable. How programs will look depends on how key stakeholders take action.

Today’s methods of identity control are superior to those implemented earlier this millennium, when security efforts were typically developed locally and had no enterprise-wide standards. Even within branches of the country’s military, installations maintained unique processes. Often, no vetting standards existed and those that did were subject to change with new leadership. Vendors and service providers typically needed multiple credentials to gain entry and even then they experienced long waits at highly congested inspection points.

Fast forward and identity management is nearly unrecognizable today. Comprehensive, standardized vetting requirements are implemented across an enterprise and privileges at multiple locations are authorized through one service. Authorized personnel are automatically and regularly re-evaluated to catch new developments. Vendors assume the expense of obtaining clearance; although security is a cost of doing business, costs are recouped through increased productivity and efficiency thanks to time savings.

By adopting a streamlined process for vetting individuals, sensitive government and commercial enterprises reduce security risks by eliminating uncertainty about who is on site. To control and improve security, however, work remains.

Identity management companies rely on fragmented information sources, with thousands of law enforcement agencies reporting activity through various systems. Congress must work to align the country’s many databases detailing criminal activity and information. Further, government agencies and military branches need better coordination in sharing no-entry lists, ensuring that a security risk to one entity is recognized elsewhere. Screening must evolve to consider unexplored background that could disqualify an individual, such as mental health. Finally, leveraging the private sector’s technological advancements will be critical to adding the highest level of security possible while closing vulnerability gaps.

Rethink your cyber strategy

E

ven the most sophisticated, well-intentioned perimeter-focused cybersecurity strategy cannot possibly be 100 percent effective — yet that’s what is required for these approaches to succeed.

Security breaches are inevitable, and the fault doesn’t lie in the quality of your perimeter defense tools or your IT security staff. The problem is your fundamental approach. The increasing interconnectedness of organizations extends the network perimeter while also making it more porous. Mobile and cloud computing push the range of enterprise applications and data far beyond the data center and provide new ways for malware to enter the network. Once inside, malware is invisible to perimeter defenses, exposing the enterprise’s “digital crown jewels” to harm.

Advanced threats are winning against current security controls, and adding more controls doesn’t help. The most dangerous threats are stealthy and persistent, often unfolding in stages over days, weeks, or even months. Attackers can remotely direct the initial compromise, causing it to spread laterally and shape-shift to achieve their end game.

Each prevention-centric product has only one imperfect chance to identify a particular threat before it slips past the defenses into the network. And once malware enters the network, perimeter defenses are blind to any further activities, leaving attackers free to conduct their dirty work.

Prevention-focused security strategies drain IT resources. It can take an experienced security analyst weeks to properly tune a firewall or IPS and hours or days to sift through thousands of daily alerts. There aren’t enough highly skilled security analysts to meet demand.

Network security has always been complex, but that complexity is accelerating — as is the sophistication of the entire ecosystem of malware. What’s needed are cybersecurity strategies that are more even more adaptive than the malware they’re trying to outmaneuver.
Like virtually all online threats, malware is increasingly finding a ripe new territory on the mobile platform, reports Karen Epper Hoffman.

At the beginning of the year, Justin Somaini gave his cybersecurity colleagues a call to arms that cited the rising threat of mobile malware. “We’re now free to work on any device, in any location, around the world,” the chief trust officer for Box, the Los Altos, Calif.-based cloud computing giant, wrote in his mid-January blog post on the company’s website. “The gains from these new technologies have been massive, from life sciences companies advancing drug research to manufacturers working with a global supply chain. But these benefits have come with a cost.”

Somaini, who held top IT security spots at Yahoo, Symantec and Verisign before coming to Box, sees the current and growing issue of malware on corporate mobile devices as a top concern for his fellow cybersecurity officers: “If we look back over the past 40 years in technology, we have seen this movie before,” he says. “We are starting to see [mobile] becoming a sizable foothold for malicious individuals with the huge upswing in mobile device usage in the past two years.”

Mobile malware has indeed become a grave concern for security pros. Last year, we saw multiple new attacks on both Android and iOS devices, namely WireLurker which attacked (supposedly more secure) non-jailbroken iOS devices. Mobile devices are ripe for attack for many reasons: They often hold user credentials for applications and websites. They’re used for out-of-band authentication. They are almost constantly connected to the internet. And they have audio and video recording capabilities. For high-profile targets, these devices are a treasure-trove of information. And mobile
People are starting to move money with mobile devices."

—Dave Frymier, VP and CISO, Unisys

MALWARE THREAT: Mitigation

In the face of heightened concern and a rising threat, how can organiza-
tions start to tame the potential for mobile malware attacks?

For Justin Somaini, chief trust officer, Box, the plan starts first with education. In order to support employees in protecting themselves and their access to mobile assets (both personal and corporate), security practitioners need a "near-world plan on driving education and culture change," he says. Information technology and support desks should regularly communicate to employees information about security updates or emerging or erroneous threats that target mobile.

Also, he says, organizations need to consider fundamental security precautions, like making sure that the company maintains a network for guest mobile users or contractors that is completely separate from the corporate network. In addition, companies need to review both their mobile device management solution providers and mobile-oriented vendors that handle application-level products and services to determine whether they are well-positioned to combat potential malware threats.

Several vendors have embraced the mobile device fundamentals profile put forth by the NSA, according to Neal Ziring, technical director, information assurance directorate, National Security Agency. But, vendors and user organizations need to focus on the fact that mobile device security must extend beyond the end-point device. "The overall architecture matters too," says Ziring. "Organizations should ask, ‘What is the potential exposure to my enterprise? How is my back end? Do I have adequate monitoring and am I protecting my most important data? The awareness of the attack surface matters a lot more.’"

While it is critical to investigate the controls on the device and application level, Deepak Rout, chief security officer for The Co-
operators Group, says that false positives must first consider the

more people are starting to use their

smartphones and tablets for work — in many cases, using their own personal devices — hacking and information thieves are drawn to the enterprise email and access to other valuable information on or retrievable through these devices.

While Ziring says that malware on legacy desktop platforms has not gone away, mobile malware is particularly concerning because of the rapid growth of the threats and because the detection and counter-measures to combat malware on mobile are not as well-established as those are on more traditional platforms. "That’s an area for the industry that is improving rapidly," Ziring says, "but it still has a ways to go."

Hot potato syndrome

When it comes to the mobile platform, there’s also the hot potato syndrome.

In other words, whose responsibility is it to manage a potential malware intrusion? Is it the network carrier, the handset maker, the operating system developer, the security vendor, the company allowing their employees to use BYOD? According to Adam Tyler, chief innovation officer for CSDT, an Austin, Texas-based provider of global identity protection and fraud detection technologies, this is just one major reason why mobile malware is "going to become so prevalent and [we will have] a huge install base that will never be patched."

"Android phones are being sold with operating systems that are analogous to Windows 98," says Randy Abrams, research director for NSS Labs, an Austin, Texas-based information security research and advisory company. Brand new devices are sold with old, less secure versions of the operating system and neither the developer, nor carriers have any interest in providing more secure versions of the OS, he explains. "The number of new mobile devices with no upgrade path to current versions of the Android OS, or future versions with better security features, is growing every day," he says. "This is a critical problem that manufacturers and carriers have no interest in addressing. Consumers tend to trust applications on smartphones without question, which makes social engineering exceptionally easy."

Even in an increasingly cybersecurity-conscious environment, it does not take much skill to trick a user into installing malware on their mobile device, says Abrams. Anti-malware vendors are at a significant disadvantage against malware as by design they are not allowed to run at root level and, unlike the malware writers, legitimate security vendors have to follow rules that preclude maximum effectiveness, he says. While some devices are shipped with one anti-malware product installed, this does not mean the installed product will be the correct choice for all users — and replacement at the root level is impossible without rooting the device.

Additionally, Tyler points out, in risks. Figuring out an organization’s mobile risk profile is “a huge gap in a world empowered by mobility," Rout says. He maintains that foundational controls are no-brainers: Organizations should deploy authentication systems to access applications, secure email data; vulnerability and patch management; monitoring and incident management; and device-level security, including password, en-
cryption and wiping on reported losses.

In the military, John R. "Rick" Walsh, mobile lead for cybersecurity, U.S. Army, says it security efforts currently focus on both the users and the ultimate targets of malware players. “A piece of malware is written ultimately for one of two purposes: either to steal information or to deny the user from accessing information," Walsh says. “So if we focus on the goal of the attacker we can better defend against the attack.”

Organizations should install a management product and lock down any mobile devices they actually own, according to Dave Frymier, VP and CISO, Unisys. And, if an employee brings their own device and installs applications supplied by their organization, he says CISOs should consider “app wrapping” technology, which allows corporate apps to live in their own software sandbox separated from a user’s personal environment on the device.

Some cybersecurity experts, such as Lysa Myers, a security researcher at ESET, believe that companies and agencies that allow users to access work with mobile devices must use more than passwords to protect access. She recom-
mends using multi-factor authentication, encrypting sensitive data in storage and in transit (especially if users are able to access network resources from public wireless network), and limiting users’ access to network resources to the minimal level that allows them to do their job.

“Mobile malware will become a much more significant problem unless we drive solutions here,” says Somani.
Mobile malware

People are starting to move money with mobile devices.”

–Dave Frymier, VP and CISO, Unisys

emerging markets, where older mobile devices are more commonplace, exploits that may have been discovered or even stamped out in the U.S. and Europe are easily propagating and may remain in place for years to come. Mobile users in these areas have limited ways to protect themselves, Tyler says, adding that the information users once accessed by laptop is just a fraction of what is now used on smartphones today.

The threat is also on the rise as “people are starting to move money with mobile devices,” says Dave Frymier, vice president and chief information security officer at Unisys, a global information technology company based in Blue Bell, Penn. Apple Pay is the latest boost to this trend in the United States, he says, but mobile malware has been a growing problem in Europe for years now. “Mobile device hygiene issues – such as weak passwords, downloading apps from questionable places, clicking on the wrong things – are the key factors predating these attacks,” Frymier explains. “This is pretty much the same list of security hygiene issues that applies to a regular PC.”

While for many CISOs, vendors and analysts, mobile malware is still relatively rare in comparison to other threats, “It’s another avenue of attack, another source of cost for IT departments,” says Frymier. And he expects the risk to only rise. “As mobile devices spread and are used for financial transactions, the amount of exploits will increase.”

Indeed, the ease of monetizing attacks makes the return on investment very attractive for would-be mobile attackers, according to Abrams. Attackers even smartphones enable attackers to circumvent some methods of two-factor authentication even when users are using their computers, he points out, and development standards for Android are free and the cost to make apps available for download is insignificant. “The ease of getting malware installed on Android phones, which is what almost all mobile malware is written for, sets a low bar for a successful attack,” Abrams says. “A lack of accountability for developers results in a low likelihood of criminal apprehension.”

Malware writing is a very lucrative endeavor, echoes Lysa Myers, security researcher at ESET, a global IT security company with U.S. headquarters in San Diego. “Criminals are able to get into phones or tablets by way of social engineering or vulnerabilities in software, especially as few people understand the importance of securing their mobile devices,” she says.

Risk management

In fact, most industry observers agree that the overall situation is likely to get worse before it gets better, especially since mobile devices – even those used to access sensitive information – are not always routinely updated, according to Ziring.

Further, Somaiya says that organizations may need to take a step back and look for new ways of dealing with this threat. While the controls around the device and the content have not changed from traditional platforms, there are definitely greater limitations on the operating system level. And conventional anti-virus approaches are not cutting the mustard in mobile.

“What we need is more vendors focused on the mobile space,” Somaiya says. In particular, new solutions need to take into account that, increasingly, employees are using their mobile devices to access corporate assets that are not necessarily resident on the device, but in the cloud, through services like Salesforce.com and Box.

Predicting attacks is a new area that organizations are just starting to investigate, according to Walsh, who, like other cybersecurity experts, is seeking to reduce if not eliminate malware’s ability to attack information. In the case of government employees’ devices, software is tested, verified and secured before it can be used. And his organization within the U.S. Army is working to establish mobile application development standards for developing and using secure applications.

“The most difficult way to predict malware is to think like the malware developers and build proactive controls and tools that allow the mobile device to have protection before it is attacked,” Walsh says. “This is, however, a change to current practice, which traditionally is a reactive posture where we wait to see what the malware does then we work to stop it.”

Deepak Rout, chief security officer for The Co-operators Group, a Canadian insurance company, admits that it is not easy to create data security architecture in the mobile world. The key, he says, lies in understanding the value of data being considered for mobility. He recommends classifying all data into multiple security classes and understanding which classes are involved in business processes enabled by mobile devices. As well, it is imperative to understand the consequences should data be exposed, and systematically develop layered controls for managing those identified risks. “So, it’s essentially the age-old risk management, but at a data level,” Rout says. “And, of course, this is hard on three levels: IT risk management is little understood, hard to implement in practice and rarely goes to the level of data.”

Federal enforcement

The Federal Trade Commission (FTC) has become the de facto enforcer of data privacy laws and regulations, reports Lee Sustar.

All them the data breach police. The Federal Trade Commission (FTC), once known primarily for chasing down flimflamers and makers of shoddy products, has transformed itself into the primary enforcer of federal law and regulations surrounding consumer privacy issues. Even as huge cybercrimes at Target, Home Depot and Sony Pictures Entertainment dominate the headlines, ongoing FTC legal actions aimed at companies like LabMD and Wyndham Worldwide Corp. – where federal courts greenlighted the agency’s enforcement authority over data breaches – may ultimately prove far more important in establishing standards for private sector protection of consumer privacy and the penalties for the failure to do so. It comes as no surprise that President Obama, in a preview of his State of the Union address, chose to announce his proposal of a national data breach law in a speech at the FTC, in which he praised the agency’s efforts.

If the FTC commissioners have their way, enterprises can expect the agency to assert itself still further in data security matters. “This is where we have seen consumers express concern,” says Maneesha Mithal, associate director, division of privacy and identity protection at the commission. “Identity theft has been the number one complaint we have received over the last decade.” She shrugs off business complaints – made perhaps most forcefully in the Wyndham case – that the FTC hasn’t given sufficient guidance to companies trying to stay on the right side of the law. She cites numerous documents as evidence, in particular, a major report on privacy concerns in the Internet of Things (IoT). FTC commissioners and staffers are often speakers at IT and
security industry events, because that’s where the GISOs are, she notes. In any case, interested parties seeking to figure out where the FTC stands can simply look it up. “We have our 53 settlements in data breach and privacy cases,” says Mithal. “Every one of them is online.” The agency’s emphasis is on procedures, not IT products or cybersecurity methods, as the agency avoids being prescriptive about what security technology should be used. “Companies need to do is to do what is reasonable,” she says.

Yet, even with the documents produced by the FTC and the federal government’s National Institute of Standards and Technology (NIST), it can still be difficult to meet the FTC’s reasonableness standard, says Mike Lloyd, chief technology officer at RedSeal, a Sunnyvale, Calif.-based security analytics firm. “The main objection from Wyndham makes a lot of sense,” he says in a written comment. “What is needed are established guidelines, so that a company can know whether they are doing what is agreed, industry-wide, to be appropriate security.”

Sooyong Cho, a former staff attorney for the FTC who is now a partner with K&L Gates, a law firm composed of more than 2,000 lawyers practicing on five continents, also emphasizes that companies must do more than conform to procedures that meet the standards of their particular industries. “The FTC has criticized companies for failing to stay on top of industry standards,” she says, such as taking adequate steps to protect their data from common attacks, like SQL injection. Yet even more explicit FTC guidelines on data security may not get to the root of the problem, says Eric Chiu, co-founder and president of HyTrust, a cloud control company with U.S. headquarters in Mountain View, Calif. The issue, he says, is that “corporations continue to put revenues ahead of security.” Until that changes, he adds, more stipulations on data and privacy from the FTC may result in more red tape for companies and higher costs for consumers.

The proposed federal data privacy law may bring clarity to the situation, says attorney Paul Paray, a partner at Zimmermann Weiser and Paray, a Westfield, N.J.-based law firm which specializes in commercial litigation services. “If the FTC’s staff weathers the storm, the adoption of a federal breach notification law with some baked-in security standards or widespread adoption of the NIST cybersecurity framework standards – or any other federal standard yet to be promulgated – may eventually provide the FTC with a repellant sought by Wyndham and others,” Paray says.

In the meantime, companies have to adjust themselves to the reality that the FTC’s authority is decisive for now. While big corporations have adapted by beefing up privacy protection and bringing in broad based legal counsel, smaller outfits hoping to make it big in the latest tech boom may be surprised that they have obligations to meet the FTC’s consumer protection standards, too. “If you are a small mobile app developer working in a garage, you may not have heard of the FTC,” says Mithal. For smaller players and big companies alike, the key to avoiding running afoul of the FTC is planning for privacy protection while products and services are still in the planning stages – what FTC Commission Chairwoman Edith Ramirez calls “security by design.”

Gary Kibel, an attorney at Davis & Gilbert, a New York-based law firm, agrees. “It is hard to remedy those issues after the fact,” he says. “You are potentially facing a lot of damage data under a flawed model.” He adds that the potential liability is “very significant.” With limited capacity, the FTC has been forced to choose its targets carefully with the apparent aim of disciplining the tech industry as a whole. High-profile actions in 2012 resulted in a $22.5 million penalty paid by Google to settle charges that it misrepresented privacy to some users to a fine-free do-over for Facebook that compelled the social media giant to obtain consent for sharing information beyond privacy settings. Google could shrug off a penalty that amounts to a rounding error in the company’s $50 billion in revenue that year. Nevertheless, the FTC’s actions against other companies, particularly in the retail and customer service sectors, are systematically reshaping the ways in which businesses collect and safeguard customer data, says Tom Smidhoffer, a partner at Edwards Wildman Palmer, a law firm with 16 offices worldwide. A milestone, he says, came in 2009 when retailer BJ’s Wholesale Club reached a consent agreement with the FTC that the company violated the law even though it made no explicit representation about, or promise to protect, customer privacy.

The BJ’s Wholesale decision, along with state laws protecting data privacy and security passed in the last decade, have created a fairly clear picture governing the protection of consumer data and personally identifying information, says Smidhoffer. “Step back from all the state laws, court cases and FTC decisions, and a pattern starts to emerge – or a trend – saying that all companies have some level of data security obligation,” he says. “At the end of the day, the obligations here may be tougher than they are in the European Union. There is just no one place to look at to come to those conclusions.”

Marcus Christian, a partner with Mayer Brown, a legal services provider, makes a similar point – and credits the FTC for driving the data protection legislative agenda at the state level and giving cues to federal law enforcement.

corporations continue to put ...profits ahead of security.”

- Eric Chiu, president, HyTrust

It is hard to remedy those issues after the fact.”

- Gary Kibel, attorney, Davis & Gilbert

The FTC’s unexpected role as top cybercop developed nearly a century after its creation in 1915 during the Woodrow Wilson administration, a few years after Upton Sinclair’s novel The Jungle shocked the country with its exposé of unsanitary and unsafe conditions in the meatpacking industry. A product of Progressive Era reforms, the FTC was charged with exposing fraud and deceptive business practices and challenging anticompetitive business mergers. The New Deal of the 1930s gave the FTC much greater prominence, as President Franklin Roosevelt personally oversaw the FTC’s role as top cybercop de-
Even when you’ve got a breach or an insider gone bad, there are still ways to limit the damage and protect data, reports Alan Earls. It’s a lesson for today’s CISO for whom security measures far more arcane and complex than a simple “Open Sesame” password are required to guard corporate treasures. Yet, as many have found, systems are always going to be breached. So, an additional focus needs to be placed on making data “exfiltration” far more difficult, whether the breach is accomplished through an insider or via undetected malware.

“Outbound traffic is the key enabler of modern attacks — it links internal malware to the outside attacker, allowing a near infinite ability for the attack to adapt and spread over time,” notes Wade Williamson, director of product marketing at Vectra Networks, a San Jose-based vendor of cyber attack detection technology. “In addition to the control functions, outbound channels represent the actual path of loss where key data and assets leave the target organization. In short, it’s the source of both harm and complexity in modern attacks,” he says.

Of course, detecting outbound traffic is just a first step. A possible symptom of data leakage is increased use of external sites and the most obvious means of detecting that leakage is to implement a network monitoring and data loss prevention (DLP) system, which can help to identify information leaking from the organization, says James Bindseil, president and CEO of Globalscape, a San Antonio, Texas-based provider of secure file transfer solutions. “More generically though, you need to make sure all of the different ways that leakage can occur are protected, and it is important that all communications mechanisms are a part of the DLP solution,” he says. For example, leveraging tools that can integrate
Data leak prevention

...you are able to build a risk profile and flag for...behavior…

— Peter Tran, RSA

“Data exfiltration is like insulating your home.”

— John Pescatore, SANS Institute

into the broader security and DLP solutions, through methods such as internet content adaptation protocol (ICAP) integration, can provide warning signs that can indicate a problem.

In fact, notes Peter Tran, senior director worldwide advanced cyber defense practice at RSA, a Bedford, Mass.-based network security company, a traditional perimeter-only defense approach is not effective any more given the overwhelming porous nature of networks today and the increasing requirement for global interconnectivity. That implies, in his view, crafting a strategy to combine different security methods. Thus, a risk-based approach to cyber defense is needed that considers which assets are most critical – with business context and a risk index tied to business impact or loss. “This approach should be implemented across multiple domain areas – such as incident response, cyber intelligence, analytic intelligence – to provide balanced capabilities across critical security operational areas in addition to traditional layered defense in-depth,” Tran explains.

He says in most cases the first priority in detecting data exfiltration or “leakage” is anchored on an intelligence-driven security strategy he calls the “cyber defense triad,” which is an organization’s capability across people, process and technology. To achieve this strategy, organizations need to have the ability to identify “people” who may be attacking and the how and why they are targeting your organization. Further, it is vital to understand the process and gain insight via host and network behavioral analytics of the attacker. This means having the right technology so that data never leaves the perimeter.

“The output of this analysis – combined with workflow and process automation – helps analysts in a security operations center (SOC) to establish a visualization of the threat infrastructure being used to compromise specific high-value areas of a given organization’s network,” Tran says. Security practitioners can then perform infrastructure takedown to disrupt these covert channels from communicating outbound, he adds.

That constitutes the basics, in Tran’s view. But there’s more, much more. He said it is also increasingly vital that organizations have the ability to monitor and detect for pre-weaponized covert channels piggybacking off legitimate outbound communications to partner or supply chain trusted connections. This is commonly referred to as the inside-out agent challenge, he notes, and it happens when an attacker takes advantage of trust relationships between multiple entities and then uses legitimate channels as “data tunnels” to exfiltrate data by way of multiple hops and dead drops, called “switch targets.”

“These inside-out agents are extremely difficult to detect due to the lack of overt network anomalies,” he says. One approach to detection in these cases is to look for smaller deviations in data communication sizes, timing, artifact lateral movements, machine to machine (M2M) role-based authentication violations and failed login attempts.

“In aggregate, you are able to build a risk profile and flag for the behavior within set parameters before successful outbound communication may occur,” he notes.

While the outside threat is paramount, insiders still represent a huge problem and can be quite easily exfiltrating data without detection while IT is focusing its energy on malware and APTs.

The “people” problem can be thought of in two ways, says Tran. People can be one of an organization’s best lines of defense as a force multiplier (human intrusion detection). With the proper end-user security awareness training they can spot and report suspicious activity. Often, before any wires are tripped. On the other hand, they can be a serious risk to social engineering cyberattacks, poor IT hygiene or actual insider threats.

“Protecting data and systems from unauthorized access while, in parallel, making the right systems available to authorized personnel is the main objective of an effective cyber defense practice,” he explains. Simple passwords and basic data protection methods are becoming less effective, so technologies such as multifactor or adaptive authentication, biometrics, out-of-band PINs and even voice callbacks are being used as external threat triage and countermeasures. “This is a risk-based approach to prevention of the people problem by aligning the right technologies to instrumentation, policy and process,” he says.

However, while technical solutions that block the transfer of data outside the organization and monitor network activity can be helpful, says Globalscape’s Bindseil, they depend on predefined policies about which type of information needs to remain internal. “This kind of solution requires a complete knowledge of the information that is classified as opposed to what is publicly consumable,” he says.

In fact, security starts with knowing what your critical data assets are, says Randy Trzeciak, the technical manager of the CERT Insider Threat Center at the Carnegie Mellon Software Engineering Institute. “If you don’t know what your data and who has access then it is hard to either detect or protect,” he says.

Thus, he notes, a solution – whether the threat is internal or external – starts with an organization implementing tools and configuring them to the environment. But, manual tagging is central to the process.

With an inventory in place and tools, such as DLP, focusing on movement within the organization or to the outside world, security pros can begin to understand what is suspicious or anomalous, he says.

Other experts warn that it is an illusion to believe that if an organization buys a security tool it will suffer no data loss as a result. “That has finally fizzled from most minds,” says Anton Chuvakin, a research vice president in risk management division at information technology research and advisory firm Gartner.

“Lately, I have spoken to people who claim that DLP cannot work at all against advanced attackers – like APT – exfiltrating stolen data,” he says. “I don’t think that is true as I am aware of examples where a DLP tool was useful for detecting such data theft by an outside party.” However, as practices for success is close involvement of business unit personnel and data owners (for all of policy definition, data classification and alert response). “Some consider this to be a foundational ingredient without which the entire DLP deployment will fail,” he says.

In other words, says Chuvakin, DLP products help protect data, not infrastructure. Thus, business unit and data owner involvement is critical at an order of magnitude more critical than other IT security projects. “Ignore it at your own peril,” he says.

Although DLP has been overhyped, it can be an important component, agrees John Pescatore, director of emerging trends at the SANS Institute. However, he thinks it is important to aim even higher – for encryption, which is perhaps the ultimate solution.

“Encryption is hard to do because it limits the free movement of data – someone on each end needs the key,” he says. “But since it may have to become more widespread, companies should consider piloting it now as a model for future control of exfiltration.”

For instance, keeping the focus on how critical data is, encryption could be used to secure sensitive communication among board members. Then, in the future, the lessons learned from this experience can gradually be applied more broadly, he says.

“Data exfiltration is like insulating your home,” Pescatore says. “There are hundreds of places where heat can leak – on top of which there are times when someone accidentally leaves the door open. So as you aim for a solution, you need to keep your eye on each of the potential leakage points.”

John Pescatore, SANS Institute

OUR EXPERTS: Stopping leaks

James Bindseil, president and CEO, Globalscape

Anton Chuvakin, research VP, security and risk management, Gartner

Peter Tran, senior director worldwide advanced cyber defense practice, RSA

Randy Trzeciak, technical manager of the CERT Insider Threat Center, Carnegie Mellon Software Engineering Institute

Wade Williamson, director of product marketing, Vectra Networks

James Bindseil, president and CEO, Globalscape

Anton Chuvakin, research VP, security and risk management, Gartner

Peter Tran, senior director worldwide advanced cyber defense practice, RSA

Randy Trzeciak, technical manager of the CERT Insider Threat Center, Carnegie Mellon Software Engineering Institute

Wade Williamson, director of product marketing, Vectra Networks
Security certifications can land you a better job, but companies are also looking for people who can communicate and manage projects, reports Steve Zurier.

There’s always a pivotal moment in a person’s career when they realize they need to become more proactive. That moment came for Todd Bell in the months following the 9-11 terrorist attacks on the World Trade Center and the Pentagon and the simultaneous dotcom implosion. Bell had been making good money for several startups during the tech boom and not long after 9-11 found himself on a low-level job at Hewlett-Packard just to pay the bills and keep food on the table for his family.

Equipped with only an undergraduate degree in business information systems, Bell knew he needed to offer prospective employers more. In the next two years he earned a Certified Information Systems Security Professional certification from (ISC)², as well as a Project Management Professional Certification from the Project Management Institute.

But he didn’t stop there. By 2004, Bell also completed a master’s in business administration (M.B.A.) from Regis University in Denver.

“I hate to say it, but the M.B.A. opened more doors than any other qualification,” he admits. “However, with the CISSP and PMP I tripled my salary and then within a few years of getting my M.B.A. I doubled my salary again. There’s no question that the M.B.A. put the CISSP and project management certifications in a different light and made me more valuable.”

Today, Bell works at California-based cybersecurity advisory company Intersec Worldwide as vice president of enterprise security, earning the top end in salary for a CISO, which is well into the six figures. He often works as a CISO for three months to a year, setting up and rebuilding teams and helping them revise their security program.

Bell’s experience maps well to what analysts, vendors and officials from the certification organizations told SC Magazine about developing a career as an IT security professional. Certifications and extra courses are important – they will land you a higher-paying, hands-on security position – but nailing down that executive-level job requires taking some extra steps.

“What companies tell us they need today are multidimensional security people who can translate technology risk into business risk and speak a language that can be digested by the people who control the funding and resources for IT security,” says Bill Reynolds, a research director at Foote Partners, which publishes IT skills demand and pay analysis reports.

“IT people often think you can just get a degree and go into management, but it’s not that easy.”

Two other certifications that can drive value to a security career are the Certified Information Systems Auditor (CISA) and the Certified Information Security Manager (CISM). But analysts say that IT security people often need more than just technical skills.

“Often the top security people are people who have been in the trenches, developing products and software, and then they move into security. They may have a product management background,” says John Pescatore, a research director at Gartner. “They have a better feel for the business and a better feel for the technology.”

The amount of value IT security certifications can add is strongly dependent on the person who has earned the certifications. Many people see their first IT certification as a stepping stone to their next career move. But others see certification as a permanent part of their professional makeup.

“Some people put a lot of effort into their security certifications and they become the go-to person for security issues,” says Reynolds. “They will have been through the wars and will have extensive experience.”

But, he adds, that also means they may have a lot of experience – and it may be time for the next step in their career.

“I think people should be looking for the next step and not just stay in the same job,” he says. “Security is a career, not a job.”
people who understand data analytics just people who can technically perform
vice president of strategy and innovation
But now managers understand that a hard to justify spending on IT security.
benchmark research drawing from
Security certifications

The test covers 10 security domains and candidates must have five years of paid full-time Computing Technology Industry Association.
dent handling, firewall and perimeter protection, forensics, hacker techniques, Windows and Unix OS security, secure software and application coding. Tests are administered by
test of a Windows security, once a year. (ISC)2 is best known for the Certified Information Systems Security Professional (CISSP).
Global Information Assurance Certification.
The average salary for an information
a SAMPLING:
IT security courses
Information Systems Audit and Control Association. ISACA offers four major certifications: Certified Information Security Auditor (CISA); Certified Information Security Manager (CISM); Certified in the Governance of Enterprise IT (CGEIT); Certified in Risk and Information Systems Control (CRISC). Costs for these certifications range from $420 to $725 for members who register online to $725 for nonmembers who register by mail after the early-bird deadline. ISACA also now offers a Cybersecurity Fundamentals Certificate for entry-level security professionals. The exam costs $150. For more information, visit isaca.org.
International Information Systems Security Certification Consortium. (ISSC)’s best known for the Certified Information Systems Security Professional (CISSP). The test covers 10 security domains and candidates must have five years of paid full-time work experience in two of the 10 domains. Standard registration for the five-day seminar is $2,695. For more information, visit issc.org.
Computing Technology Industry Association. CompTIA’s Security+ certification is geared for IT workers looking to secure the following job titles: security engineer, security consultant, network administrator, IT security manager. The test costs $293. CompTIA also offers the Advanced Security Analyst, which leads to positions as an IT specialist in InfoSec, risk manager/analyst, security architect, penetration tester/ethical hacker. Cost for the exam is $395. For more information, visit comptia.org.
Global Information Assurance Certification. GIAC offers some of the best hands-on courses available. Topics range from security audits, intrusion detection, incident handling, firewall and perimeter protection, forensics, hacker techniques, Windows and Unix OS security, secure software and application coding. Tests are administered by the SANS Institute. The five-day Intro to Information Security course costs $4,395. Single days are available. For more information, visit giac.org and sans.org.

A SAMPLING: IT security courses

Security certifications

Security professional can’t keep their head above water in the business, and the cloud has forced IT departments to think more like data architects who can develop a holistic view of the organization and apply security policies across the organization. As part of this, they have to develop remediation plans in the event of an attack.

Understand mobility and the cloud. The cloud has forced IT departments away from the upstairs fortress, and mobility has accelerated the trend even further. More IT security workers may wind up working for Amazon Web Services and Microsoft Azure as opposed to working in IT departments at companies. And security professionals need have a good working knowledge of mobile device management and mobile application management.

B
based on interviews with analysts, products vendors and certification organizations, here are five must-have IT security skills.

Computing Technology Industry Association. CompTIA’s Security+ certification is geared for IT workers looking to secure the following job titles: security engineer, security consultant, network administrator, IT security manager. The test costs $293. CompTIA also offers the Advanced Security Analyst, which leads to positions as an IT specialist in InfoSec, risk manager/analyst, security architect, penetration tester/ethical hacker. Cost for the exam is $395. For more information, visit comptia.org.

Global Information Assurance Certification. GIAC offers some of the best hands-on courses available. Topics range from security audits, intrusion detection, incident handling, firewall and perimeter protection, forensics, hacker techniques, Windows and Unix OS security, secure software and application coding. Tests are administered by the SANS Institute. The five-day Intro to Information Security course costs $4,395. Single days are available. For more information, visit giac.org and sans.org.

Security certifications

benchmark research drawing from 2,700 employers. “In the past, it’s been hard to justify spending on IT security. But now managers understand that a security incident can cost them market share, which is why people who can communicate the need for IT security are extremely valuable today.”

Robert Stroud, recently elected the international president of ISACA and vice president of strategy and innovation at CA Technologies, agrees with Reynolds that it takes more than security knowledge alone to be effective today. “We need people who can look for unusual and unplanned behaviors, not just people who can technically perform monitoring,” he says. “And we also need people who understand data analytics and the business outcomes of exposures to security incidents. Security profession- als today have to presume that security incidents will occur.”

Focused certifications

That’s not to say that people who simply enjoy hands-on tech work looking for career growth can’t find it in the IT security industry. There’s no question that there’s great opportunity out there. Cisco’s “2014 Annual Security Report” estimates that as of this year the industry has a shortage of one million security workers worldwide. The shortage has resulted in companies offering excellent salaries for people with the right qualifications.

Foote Partners reports that for the six-month period from Jan. 1, 2014 to July 1, 2014, market value went up 42.9 percent for a GIAC Certified Penetration Tester, 33.3 percent for a CWNP Certified Wireless Network Administrator (CWNA) and 25 percent for a GIAC Exploit Researcher and Advanced Penetration Tester. “People are paying attention to workers with the right qualifications,” says Reynolds of Foote Partners. “Penetration testers, auditors and even those with wireless security skills are getting noticed.”

Meanwhile, CompTIA reports that 53 percent of IT workers would like to further develop their security skills in the next two years. And for good reason. The average salary for an information security analyst is $86,170 – and workers who combine the security training with advanced degrees or specialties in IT architecture or data analytics can easily command six-figure salaries.

Almost everyone we talked to agrees that there’s a fundamental shift in how IT departments look at security capabilities.

Tom Gilheany, product manager at Learning@Cisco, says in the past, security professionals have to think more about a simulated security incident. “There’s a big question today as to whether or not we are getting on top of the problem with security incidents,” Tomic says. “This new certification is for people who want to take on the first-responder role and actually work on networks that have been attacked. It’s about taking the big picture, because that’s what won’t go away.”

Other certification groups have responded with courses that seek to develop skills for responding to security attacks. In October, GIAC announced a new certification, the GIAC Network Forensic Analyst (GNAF), which will teach students how to analyze the network following a hacking or security incident. The GNAF certification will be released in early November and pre-registration is now available with the SANS Institute’s Advanced Network Forensics and Analysis course.

D’Arcy Davis, technical director at GIAC, says that students who successfully complete the certification will have demonstrated that they have the capability of collecting and filtering evidence of abnormal or malicious activity from diverse network sources such as log files and network packet

Top IT skills IT professionals plan to pursue

Security skills: 5 must-haves
B

Security professionals need have a good working knowledge of mobile device management and mobile application management.

---

SECURITY SKILLS: 5 must-haves

Based on interviews with analysts, products vendors and certification organizations, here are five must-have IT security skills.

Computing Technology Industry Association. CompTIA’s Security+ certification is geared for IT workers looking to secure the following job titles: security engineer, security consultant, network administrator, IT security manager. The test costs $293. CompTIA also offers the Advanced Security Analyst, which leads to positions as an IT specialist in InfoSec, risk manager/analyst, security architect, penetration tester/ethical hacker. Cost for the exam is $395. For more information, visit comptia.org.

Global Information Assurance Certification. GIAC offers some of the best hands-on courses available. Topics range from security audits, intrusion detection, incident handling, firewall and perimeter protection, forensics, hacker techniques, Windows and Unix OS security, secure software and application coding. Tests are administered by the SANS Institute. The five-day Intro to Information Security course costs $4,395. Single days are available. For more information, visit giac.org and sans.org.

Computing Technology Industry Association. CompTIA’s Security+ certification is geared for IT workers looking to secure the following job titles: security engineer, security consultant, network administrator, IT security manager. The test costs $293. CompTIA also offers the Advanced Security Analyst, which leads to positions as an IT specialist in InfoSec, risk manager/analyst, security architect, penetration tester/ethical hacker. Cost for the exam is $395. For more information, visit comptia.org.

Global Information Assurance Certification. GIAC offers some of the best hands-on courses available. Topics range from security audits, intrusion detection, incident handling, firewall and perimeter protection, forensics, hacker techniques, Windows and Unix OS security, secure software and application coding. Tests are administered by the SANS Institute. The five-day Intro to Information Security course costs $4,395. Single days are available. For more information, visit giac.org and sans.org.
Security certifications

Companies want a comprehensive approach...

― Danny Tomic, Learning@Cisco

“Those are pretty high-level skills,” says Davis. “Somebody coming into this course has to have a fair amount of programming background, as well as a good foundation of security skills.”

Finding a niche

The recent overhaul of the health care system under the Affordable Care Act combined with the increased use of electronic medical records has created a tremendous need for more experienced IT security professionals in the medical field.

In response to the growing need, (ISC)2 developed the Healthcare Information Security and Privacy Practitioner (HCISPP) certification, a course that’s geared to many health care workers, including compliance officers, information security managers, medical records supervisors and risk analysts.

“This course is for anybody in the medical field who touches medical data,” says Rae Hayward, senior manager, product development at (ISC)².

The course covers six domains: the health care industry, regulatory environment, privacy and security, information governance and risk management, information risk assessment, and third-party risk management.

“We cover the ins and outs of how medical data affects health care,” she says. “We teach people how to write appropriate policies and procedures and how to have risk analysis and assess them in place.”

With so much at stake in the job market and people’s personal career growth, James Stanger, senior director, product development at CompTIA, says whichever path a security pro takes, they must understand that they are working in an increasingly complex attack surface.

The threat landscape has changed dramatically in the last three to five years. “Security workers also need to understand the cloud and how to work with BYOD and mobile devices,” he says. “But the main issue is to understand the sophistication of the hackers as well as the devices. As we automate with robotics and build smart homes, a worm or virus can attack those systems as well.”

And that’s when the project management skills that Todd Bell developed become so important. Moving forward, security professionals will be expected to roll out a security program and put all the pieces together.

Companies want security. And they want the whole package.

― James Stanger, senior director, product development at CompTIA.

FED ASSISTANCE: Excellent idea

The federal government knows that it needs to attract young people into the IT security field, both to work in government and private business at large.

Ernest McAffee, lead of National Institute of Standards and Technology (NIST), who heads the National Initiative for Cybersecurity Education (NICE), says as part of the NICE program the National Security Agency and the Department of Homeland Security designated 44 institutions as NSA/DHS National Centers of Academic Excellence in Information Assurance/Cyber Defense.

The academic excellence program was started in 1998 by NSA. DHS became a partner in 2004 and four years ago a two-year program was added. Participating institutions range from Carnegie Mellon and California Polytechnic University, Pomona, to a two-year degree program in information assurance at Prince George’s Community College in Maryland.

McAffee says scholarship money is available, though students who accept scholarships must agree to a two-year slot with the federal government before they move on to the private sector.

“The program has been extremely successful,” he says. “In the history of the program we’ve recorded a 94 percent graduation rate.”

For more information, visit https://www.nsa.gov/ia/academic_outreach/nat_cae/.

A deeper dive into vulnerability management

Welcome to our annual rundown of vulnerability management tools. This is an interesting category as much for its stability as its evolution. For example, the traditional approach to vulnerability management is test, patch and test some more. That still happens, but the evolving trend is to test constantly and remediate as you go.

So the basic idea of the test/remediation cycle still is with us, but it isn’t quite your grandparental vulnerability management either. The reason, of course, is that the whole idea of vulnerability has changed. Today, the traditional issue of unpatched devices, while still a huge problem, has to share vulnerability space with sophisticated malware. There is a myth that most, if not all, breaches are caused by malware. Actually, some of the worst attacks start with a manual incursion into a vulnerable edge device. The problem is then exacerbated by a skilled insertion of appropriate – and usually custom – malware. The purpose of this usually is to exfiltrate data or to provide a back door for the attacker to use to return. This usually is not an attack of opportunity as are many pure malware-based attacks. This is targeted and very specific to the victim. So here is where we start thinking about the different forms that vulnerability can take.

Certainly there is vulnerability in the unpatched server that admitted the attacker in the first place. But very often a bigger vulnerability exists in the network architecture itself. This is not something you can patch. When an organization places a development server web on the network with direct access from the internet, it is an open invitation for an intrusion. These devices often are not carefully secured. Rather, they often provide a clear path into the network. If the developers are using live instances of backend databases for testing, it is even worse.

This month, we take a close look at some excellent vulnerability management tools – and not all of them are restricted to the traditional types of vulnerabilities. There are several familiar players here – vendors we’ve seen for years. But like the vulnerabilities they manage, these are not your legacy vulnerability assessment tools.

Testing and reviewing was carried out by our trusty SC Lab team of Sal Picheria, Ben Jones and James Verderico. – Peter Stephenson

BeyondTrust

A powerful network security tool

P36

Rapid 7

A comprehensive vulnerability scanner

P39

Skybox

Enterprise vulnerability assessment

P42

How we test and score the products

Our testing team includes SC Labs staff, as well as external experts who are respected industry-wide. In our Group Tests, we look at several products around a common theme based on a pre-determined set of SC Labs standards (Performance, Ease of use, Features, Documentation, Support, and Value for money). There are roughly 50 individual criteria in the general test process. These criteria were developed by the lab in cooperation with the Center for Regional and National Security at Eastern Michigan University. We developed the second set of standards specifically for the group under test and use the Common Criteria (ISO 15488) as a basis for the test plan. Group Test review 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 technol-

gy 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

Our 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 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.


What the recognition means

Best Buy goes to products the SC Labs rates as outstanding. Recommended means the product has shown in a specific area. Lab Approved is awarded to extraordinary standouts that fit into the SC Labs environment, and which will be used subsequently in our test bench for the coming year.
Vulnerability management

To manage risk, we need to understand what vulnerabilities are in the enterprise, says Peter Stephenson.

T
his month we are examining vulnerability management tools. This has been an interesting category for several years. The history behind some of these tools, as well as how they have been used, both currently and historically, could be a column all by itself. Briefly, the genre of vulnerability management started with simple vulnerability management.

And that, arguably, started when, back in 1995, Dan Farmer and Wietse Venema wrote “Improving the Security of Your Site by Breaking Into it.” Farmer had written SATAN (Security Analysis Tool for Auditing Networks) and many of the functions of SATAN were described in the paper. At some point, someone wrote a version of SATAN called SAINT that did pretty much the same thing — and vulnerability testing was on its way to the mainstream. The idea of this type of security testing was pretty radical for the time and it was by no means embraced universally.

The paradigm at that time was running scripts against the perimeter and the devices on the network with the idea of compromising them and raising privilege levels to root. There was a real distinction made between vulnerability management and penetration testing. Vulnerability management evolved to vulnerability scanning, and penetration testing remained largely manual for some time. Then a new wrinkle appeared in the form of patch management. Patch management matured into a unique approach with its own tools and processes/procedures/automation. It was inevitable that those three pillars of vulnerability management — a term coined when they converged — would become a mainstay of ensuring security of the enterprise.

Now, let’s take a little side trip into the realm of risk. Risk consists, in one combination or another, depending on who you ask, of threats, vulnerabilities and countermeasures. While we tend to think of threats as a synonym for malware, the reality is that malware is just one of many tools used by a threat agent. Manual hacking, denial-of-service attacks, certain types of phishing that do not include malware and, yes, malware — all are tools the bad guys can use to execute a threat against a network. Vulnerabilities are those weaknesses against which the threat actor focuses. What is a vulnerability to a particular strain of malware may not be a vulnerability to a manual hack.

So, when we want to manage vulnerabilities we are, in a sense, managing risk. To do that, we need to understand what vulnerabilities are in the enterprise. Those can be unpatched systems, malware waiting calmly to harvest and exfiltrate credit card numbers, a weakness in the network architecture that allows penetration from the perimeter to the internals of the network, or a weak administrator password on a database. So, the whole idea of vulnerability scanning, penetration testing and patch management has become considerably more complicated since the early days of SATAN.

Manual penetration testing has given way to automated pen testing and there are several tools that facilitate that practice. But, still, a good current knowledge of vulnerabilities is necessary. We can get around that by using passive vulnerability scanning. Passive scanning watches data flows and figures out what should not be happening and what sorts of vulnerabilities — especially misconfigurations — would be at the root of incorrect flows.

Now, we add patch management. At some level, patch management can become very difficult on large enterprises. For that reason it needs to be automated. It also needs to be prioritized. That means that we need to patch the most egregious vulnerabilities first. We want to patch them all, of course, but a triage approach is good also. Therein lies the marriage of vulnerability testing and patch management. Asset criticality is a key issue as well.

This month we were fortunate enough to see examples of tools that do all of these things and we think you’ll enjoy seeing what the current state of the vulnerability management art is.
BeyondTrust UVM20 Security Management Appliance

T he BeyondTrust UVM20 Security Management Appliance is the preconfigured hardware offering of Retina CS Enterprise Vulnerability Management. While we tested their hardware appliance, Retina CS is also available as a standalone software installer for deployment flexibility. The physical device we received encompasses both parts of the Enterprise Vulnerability Management suite. The first part is the network scanner, which checks the network for vulnerabilities. The second part is Beyond Insight, which is the central management point for all network scanners organization wide. Using this technology, vulnerability scanning can be scaled out to encompass the entire enterprise and still be managed from one place.

BeyondTrust sent us their physical device offering for review. After we removed it from the box, we installed it in our rack with the provided mounting hardware. We connected a keyboard, monitor and mouse as well as power and turned it on. Using the front panel of the device, we configured the management interface settings and connected to the web-based management interface. Here, we configured a few basic environment settings, such as the administrator password and time settings. After that, we set up our license keys and the system performed an automatic update.

Beyond Insight is extremely powerful but takes quite some time to master fully. The web interface is very detailed with many statistics and graphs throughout. Enterprise Vulnerability Management is an extremely powerful tool. In addition to its vulnerability scanning capabilities, Retina CS can also perform privilege management for windows out of the box and can be expanded to perform privilege management on UNIX and Linux, as well as password management worldwide.

In addition to the device, we also received a quick-start booklet and a rack-install guide. The quick-start guide was a brief packet which covered basic setup. The documentation was clear and included screen shots throughout. For the physical appliance that we received, in addition to a 1,000-asset license, the cost of the unit was $24,995. This included the first year of licensing and hardware maintenance costs as well. BeyondTrust does its licensing based on the number of assets to scan, each of which can have more than one IP address. Standard aid includes eight-hours-a-day/five-days-a-week support for the first year. Support is available 24/7.

Retina CS is a powerful network security tool but it is slightly more pricey than other alternatives. The initial $24,995 price tag is steep, but the superb performance and scalable nature of this product means that fewer can be used to cover an entire worldwide network. This, combined with its privilege and password management capabilities, makes it a good value for the price.

Core Security Core Insight

C ore Security’s Core Insight is the gold standard for penetration testing and vulnerability assessment. It both scans and pen-tests on its own, but also aggregates data from other sources, like Qualys, Nessus and many others. Its standout features — annual pen-tests, suggested attack paths analysis of pivots, as well as putting pivots in the tested computers themselves — really separates Insight from other products in this category.

Core Security gave us a VM in a test environment. This VM was able to quickly draw up a full network map, so it was easy to familiarize ourselves with a completely new environment. There was some training which computers can be pivoted off of, and important ones. The tool does this by figuring down 12,000 vulnerabilities to about 80 absolutely need to fix. In our case, we had narrowed down 12,000 vulnerabilities to about 80 important ones. The tool does this by figuring out which computers can be pivoted off of, and where they can pivot to, favoring the shorter paths to the more critical infrastructure. The time saved by narrowing vulnerabilities down gives a place to start securing the network.

Insight includes a manual pen-test mode, for those who would like more than just a few scans. Scanners can pick up false alarms — every one of them does — and nothing tests a vulnerability quite like exploiting it does. Core Insight has a massive database of exploits of its own, as well as support for third-party exploits, all from a web interface. The manual pen-test is as simple as point-and-click, anyone could do so with very little experience. It made pivoting and following the suggested attack paths seem like child’s play.

The purchase of Core Security’s Core Insight costs $66,000 for the Virtual Machine with support for 1,000 assets and two remote auditors, and $10,000 per each hardware appliance, then 18 percent on top of that for support for the first year. Support is available 7 a.m. to 7 p.m. five days a week, as well as a 24/7 forum and access to private and custom-only training sessions and free upgrades.

Core Insight is the most feature-rich product we’ve tested. However, it was the most expensive product as well, and is most effective when paired with other vulnerability scanners. That said, Core Insight is worth every penny. It is a premium product with no compromises made, and an absolute pleasure. It was a clear choice to make this our Recommended product.
Qualys Express Lite

Qualys Express Lite is a cloud-based vulnerability assessment tool intended for small businesses. This product is purchased as a cloud service, whose primary purpose is to audit the external perimeter of small business networks. For small IT operations, this offers the most value for the money because internet-facing web, email and application servers are the most frequent targets for hackers. Qualys Express Lite can be extended into the internal network by way of a preconfigured virtual or physical appliance for additional cost. Virtual appliances are available for VMware, Hyper-V and Amazon EC2. Qualys Express Lite provides administrators with all necessary tools to help track, monitor and mitigate vulnerabilities.

The tool was extremely easy to set up. For our evaluation, we were provided with access to a virtual scanner appliance. Because this is a cloud-based product, all that is needed to set up the system is a workstation with a web browser and internet access. We navigated to the website where we were prompted to log in with our credentials. After logging in, we downloaded the virtual scanner appliance for vCenter and deployed it on our system. The setup ran extremely smoothly and took less than 15 minutes to download, install and completely integrate the virtual scanner device into our network. Once we configured the network settings of our virtual scanner device, basic configuration was complete.

The product comes with an exceptional feature set at an even more exceptional pricepoint. After setup was complete, we ran an inventory scan on our test network. This helped us identify active hosts and returned the IP address as well as basic information about the hosts. From the scan results we were able to compile our identified hosts into custom asset groups. The scans are extremely simple to set up but cannot be run in parallel, trying to create additional scans simply adds them to the queue. Another very interesting feature of this solution is its map capability. This allowed us to create an interactive radial or tree-view mapping of our network, which was then available for download in various file formats. Its feature set also includes continuous monitoring functionality as well as a malware detection service, which is capable of web application scanning and uses an up-to-date “zero-day” malware database.

Qualys Express Lite is a great product. It is evident that the company values its customers highly and stands behind its product because of its exceptional support offerings. This cloud-based vulnerability management tool is an absolute necessity for all small businesses, especially those with a limited budget. Not only will you get the security needed, but you will also reap the benefits of its vast feature set. This offering is more than enough to provide organizations with the necessary security to safely and confidently conduct business.

Rapid7 Nexpose Ultimate Appliance

Rapid7 Nexpose Ultimate is a comprehensive vulnerability scanner that is determined to convince you of its findings. Operating in conjunction with Metasploit Pro, vulnerability data is ready to be imported the moment that scanning is finished. After logging into Metasploit, users can quickly validate vulnerabilities by actually attempting to exploit them. In addition to the hardware appliance we received, Ntopx is also available as a software package.

We tested the physical appliance offering, which arrived in the form of a 2U server. We removed it from the box and quickly mounted it in our rack using the included hardware. We connected it to power, as well as our keyboard, mouse, and monitor. After that, we powered it on and waited a few minutes for it to start up. After connecting the management interface to our test network, we used the onboard Linux shell to configure the device for our lab network. Then, we logged into the browser-based management console using the provided credentials to complete setup. Overall, setup was very fast and was completed with no hiccups.

We tested the physical appliance offering, which arrived in the form of a 2U server. We removed it from the box and quickly mounted it in our rack using the included hardware. We connected it to power, as well as our keyboard, mouse, and monitor. After that, we powered it on and waited a few minutes for it to start up. After connecting the management interface to our test network, we used the onboard Linux shell to configure the device for our lab network. Then, we logged into the browser-based management console using the provided credentials to complete setup. Overall, setup was very fast and was completed with no hiccups.

After logging in, we were immediately greeted with a well-designed and sophisticated web user interface. Configuring the device to run scans on our network was very quick. We had the IP address as well as basic information about the hosts. From the scan results we were able to compile our identified hosts into custom asset groups. The scans are extremely simple to set up but cannot be run in parallel, trying to create additional scans simply adds them to the queue. Another very interesting feature of this solution is its map capability. This allowed us to create an interactive radial or tree-view mapping of our network, which was then available for download in various file formats. Its feature set also includes continuous monitoring functionality as well as a malware detection service, which is capable of web application scanning and uses an up-to-date “zero-day” malware database.

Qualys Express Lite is a cloud-based vulnerability assessment tool intended for small businesses. This product is purchased as a cloud service, whose primary purpose is to audit the external perimeter of small business networks. For small IT operations, this offers the most value for the money because internet-facing web, email and application servers are the most frequent targets for hackers. Qualys Express Lite can be extended into the internal network by way of a preconfigured virtual or physical appliance for additional cost. Virtual appliances are available for VMware, Hyper-V and Amazon EC2. Qualys Express Lite provides administrators with all necessary tools to help track, monitor and mitigate vulnerabilities.

The tool was extremely easy to set up. For our evaluation, we were provided with access to a virtual scanner appliance. Because this is a cloud-based product, all that is needed to set up the system is a workstation with a web browser and internet access. We navigated to the website where we were prompted to log in with our credentials. After doing so, we downloaded the virtual scanner appliance for vCenter and deployed it on our system. The setup ran extremely smoothly and took less than 15 minutes to download, install and completely integrate the virtual scanner device into our network. Once we configured the network settings of our virtual scanner device, basic configuration was complete.

The product comes with an exceptional feature set at an even more exceptional pricepoint. After setup was complete, we ran an inventory scan on our test network. This helped us identify active hosts and returned the IP address as well as basic information about the hosts. From the scan results we were able to compile our identified hosts into custom asset groups. The scans are extremely simple to set up but cannot be run in parallel, trying to create additional scans simply adds them to the queue. Another very interesting feature of this solution is its map capability. This allowed us to create an interactive radial or tree-view mapping of our network, which was then available for download in various file formats. Its feature set also includes continuous monitoring functionality as well as a malware detection service, which is capable of web application scanning and uses an up-to-date “zero-day” malware database.

Qualys Express Lite is a cloud-based vulnerability assessment tool intended for small businesses. This product is purchased as a cloud service, whose primary purpose is to audit the external perimeter of small business networks. For small IT operations, this offers the most value for the money because internet-facing web, email and application servers are the most frequent targets for hackers. Qualys Express Lite can be extended into the internal network by way of a preconfigured virtual or physical appliance for additional cost. Virtual appliances are available for VMware, Hyper-V and Amazon EC2. Qualys Express Lite provides administrators with all necessary tools to help track, monitor and mitigate vulnerabilities.

The tool was extremely easy to set up. For our evaluation, we were provided with access to a virtual scanner appliance. Because this is a cloud-based product, all that is needed to set up the system is a workstation with a web browser and internet access. We navigated to the website where we were prompted to log in with our credentials. After doing so, we downloaded the virtual scanner appliance for vCenter and deployed it on our system. The setup ran extremely smoothly and took less than 15 minutes to download, install and completely integrate the virtual scanner device into our network. Once we configured the network settings of our virtual scanner device, basic configuration was complete.

The product comes with an exceptional feature set at an even more exceptional pricepoint. After setup was complete, we ran an inventory scan on our test network. This helped us identify active hosts and returned the IP address as well as basic information about the hosts. From the scan results we were able to compile our identified hosts into custom asset groups. The scans are extremely simple to set up but cannot be run in parallel, trying to create additional scans simply adds them to the queue. Another very interesting feature of this solution is its map capability. This allowed us to create an interactive radial or tree-view mapping of our network, which was then available for download in various file formats. Its feature set also includes continuous monitoring functionality as well as a malware detection service, which is capable of web application scanning and uses an up-to-date “zero-day” malware database.

Qualys Express Lite is a cloud-based vulnerability assessment tool intended for small businesses. This product is purchased as a cloud service, whose primary purpose is to audit the external perimeter of small business networks. For small IT operations, this offers the most value for the money because internet-facing web, email and application servers are the most frequent targets for hackers. Qualys Express Lite can be extended into the internal network by way of a preconfigured virtual or physical appliance for additional cost. Virtual appliances are available for VMware, Hyper-V and Amazon EC2. Qualys Express Lite provides administrators with all necessary tools to help track, monitor and mitigate vulnerabilities.

The tool was extremely easy to set up. For our evaluation, we were provided with access to a virtual scanner appliance. Because this is a cloud-based product, all that is needed to set up the system is a workstation with a web browser and internet access. We navigated to the website where we were prompted to log in with our credentials. After doing so, we downloaded the virtual scanner appliance for vCenter and deployed it on our system. The setup ran extremely smoothly and took less than 15 minutes to download, install and completely integrate the virtual scanner device into our network. Once we configured the network settings of our virtual scanner device, basic configuration was complete.

The product comes with an exceptional feature set at an even more exceptional pricepoint. After setup was complete, we ran an inventory scan on our test network. This helped us identify active hosts and returned the IP address as well as basic information about the hosts. From the scan results we were able to compile our identified hosts into custom asset groups. The scans are extremely simple to set up but cannot be run in parallel, trying to create additional scans simply adds them to the queue. Another very interesting feature of this solution is its map capability. This allowed us to create an interactive radial or tree-view mapping of our network, which was then available for download in various file formats. Its feature set also includes continuous monitoring functionality as well as a malware detection service, which is capable of web application scanning and uses an up-to-date “zero-day” malware database.

Qualys Express Lite is a cloud-based vulnerability assessment tool intended for small businesses. This product is purchased as a cloud service, whose primary purpose is to audit the external perimeter of small business networks. For small IT operations, this offers the most value for the money because internet-facing web, email and application servers are the most frequent targets for hackers. Qualys Express Lite can be extended into the internal network by way of a preconfigured virtual or physical appliance for additional cost. Virtual appliances are available for VMware, Hyper-V and Amazon EC2. Qualys Express Lite provides administrators with all necessary tools to help track, monitor and mitigate vulnerabilities.

The tool was extremely easy to set up. For our evaluation, we were provided with access to a virtual scanner appliance. Because this is a cloud-based product, all that is needed to set up the system is a workstation with a web browser and internet access. We navigated to the website where we were prompted to log in with our credentials. After doing so, we downloaded the virtual scanner appliance for vCenter and deployed it on our system. The setup ran extremely smoothly and took less than 15 minutes to download, install and completely integrate the virtual scanner device into our network. Once we configured the network settings of our virtual scanner device, basic configuration was complete.
GROUP TEST  Vulnerability management

SAINT Security Suite

The SAINT Security Suite is a robust software package that quickly and easily gives a heads-up view of vulnerabilities on the network. The SAINT Security Suite can be purchased as a standalone software package or it can be bought as a preconfigured hardware appliance. Regardless of how it is purchased, the offering can be deployed as a scanner, a manager or both. Because of this design, one SAINT Manager can control many scanners. This allows organizations to leverage multiple installations to scan large, complex networks quickly. This, combined with the intuitive SAINT user interface lets administrators easily audit ensure compliance organization-wide from one place.

The SAINTbox appliance we received was easy to set up. After we removed it from the box, we installed it in our rack and connected a keyboard, mouse and monitor to the device. We powered it on and were greeted with a simple, text-based startup wizard that brought us through the initial device configuration. We configured the management interface and other basic organization information before we installed the license key and our email address, clicking the link and clicking through to Secunia’s servers. The Corporate Software Inspector includes a Personal Software Inspector (PSI).

Setup is a breeze for all agents. The Android app is required for putting in an email address, clicking the link and clicking install. Secunia initiated a scan and said the apps on the device were up to date and gave us a system score of 100 percent. The interface was clean and simple. The Windows app was a little more eventful. It was easy to download and install, the PSI version reports only the most critical apps to the server side. The Windows app was surprisingly snappy, as it scanned through our IT, nearly full, slow laptop drive in under 60 seconds. It found applications we had completely forgotten about, some not updated, and provided a helpful link to the update. Or in many cases, a click was enough to update the product all on its own.

The CSI app is command line install, making it easy to roll out to large deployments. Plus, it reports back to the Secunia server. It works on Windows, Mac OS X and Red Hat Enterprise Linux. Secunia makes it easy to see which of your computers need updates and can separate the data per domain, making it painless to sort and find computers, as well as assess and highlight any zero-day vulnerability programs or patches. When a required patch is found, Secunia makes it easy to see every computer on the network that needs that patch.

While the interface itself was extremely simple and intuitive, it didn’t wow us with how good it looked. But that works both ways. The interface was so intuitive and well-thought-out that we never once found ourselves looking toward the documentation wondering how to do something. The documentation was well-written in and of itself. It was clear and concise with plenty of screenshots and diagrams explaining the ins and outs of CSI.

Support options are standard and enterprise. Standard includes a setup call and email assistance with a two-day response time. Enterprise support includes full solution setup, implementation support, and telephone and email support with a one-day response time. Secunia Corporate Software Inspector is a fantastic option if you’re looking for patch management with security in mind. The Zero-Day Vulnerability support is where CSI really gets its value. CSI can really save your IT department time, money and risk, especially when it comes to zero-day vulnerabilities.

Secunia Corporate Software Inspector (CSI)

Secunia Corporate Software Inspector (CSI) inspects software on any Windows or Android device with an agent. As well as it has a network-scanning agent. These agents check for out-of-date and vulnerable programs or applications and report back to Secunia’s servers. The Corporate Software Inspector includes a Personal Software Inspector (PSI).

Setup is a breeze for all agents. The Android app is required for putting in an email address, clicking the link and clicking install. Secunia initiated a scan and said the apps on the device were up to date and gave us a system score of 100 percent. The interface was clean and simple. The Windows app was a little more eventful. It was easy to download and install, the PSI version reports only the most critical apps to the server side. The Windows app was surprisingly snappy, as it scanned through our IT, nearly full, slow laptop drive in under 60 seconds. It found applications we had completely forgotten about, some not updated, and provided a helpful link to the update. Or in many cases, a click was enough to update the product all on its own.

The CSI app is command line install, making it easy to roll out to large deployments. Plus, it reports back to the Secunia server. It works on Windows, Mac OS X and Red Hat Enterprise Linux. Secunia makes it easy to see which of your computers need updates and can separate the data per domain, making it painless to sort and find computers, as well as assess and highlight any zero-day vulnerability programs or patches. When a required patch is found, Secunia makes it easy to see every computer on the network that needs that patch.

While the interface itself was extremely simple and intuitive, it didn’t wow us with how good it looked. But that works both ways. The interface was so intuitive and well-thought-out that we never once found ourselves looking toward the documentation wondering how to do something. The documentation was well-written in and of itself. It was clear and concise with plenty of screenshots and diagrams explaining the ins and outs of CSI.

Support options are standard and enterprise. Standard includes a setup call and email assistance with a two-day response time. Enterprise support includes full solution setup, implementation support, and telephone and email support with a one-day response time. Secunia Corporate Software Inspector is a fantastic option if you’re looking for patch management with security in mind. The Zero-Day Vulnerability support is where CSI really gets its value. CSI can really save your IT department time, money and risk, especially when it comes to zero-day vulnerabilities.
Skybox Security

Skybox View Enterprise Suite

The Skybox View Enterprise Suite is an enterprise vulnerability assessment tool that is deployed to aid in vulnerability and threat management, as well as security policy management. It can be bought as a preconfigured hardware appliance, preconfigured VM or as a standalone software package for custom deployment. The vulnerability and threat management aspect allows for a continuous view of vulnerabilities on a network and provides security teams with remediation strategies to minimize risks. This is all done with the device’s automated risk analytics capability, which provides security teams with information in reducing network exposure and monitoring remediation efforts. The security policy management aspect allows network security controls to be monitored and ensures that the network maintains compliance.

The Skybox View Enterprise Suite was easy to set up. After it was removed from the box, we easily installed it into our server rack using the included rack mount hardware. After that, we connected our keyboard, monitor and mouse to the back of the server and powered the device on. After the machine booted, we configured it using the built-in configuration tool. We experienced some difficulties with the network configuration, which took us some time to troubleshoot. After we confirmed the problem was not caused by our test equipment we rebooted and were able to continue. From that point on we continued without any further issues.

The product comes with a preconfigured demo model that allowed us to test the provided mock network data. This was a useful tool that showcased a lot of the product’s advanced functionality. After viewing this we integrated the device into our test network to try it out for ourselves. We then conducted vulnerability and compliance scans on our network. These results gave us in-depth information about what systems were vulnerable, which vulnerabilities were exploitable, and ways to remediate these issues.

The Skybox Appliance Setup Guide was streamlined and contained screen shots of the step-by-step process to get Skybox running. However, the guide does not mention the necessity to reboot the system after assigning an IP address.

The Skybox View Enterprise Suite does not offer no-cost customer support. The company does provide both eight hours a day five days a week and 24/7 service, though the price is calculated based on the licensing cost of the software. Several options for fee-based options are available.

The Skybox View Enterprise Suite is easy to install. After we connected the supplied flash drive, we simply ran the installer and waited for it to install the software into our test network. We configured basic logon information with the network configuration, which took us some time to troubleshoot. After we confirmed the problem was not caused by our test equipment we rebooted and were able to continue. From that point on we continued without any further issues.

The product comes with a preconfigured demo model that allowed us to test the provided mock network data. This was a useful tool that showcased a lot of the product’s advanced functionality. After viewing this we integrated the device into our test network to try it out for ourselves. We then conducted vulnerability and compliance scans on our network. These results gave us in-depth information about what systems were vulnerable, which vulnerabilities were exploitable, and ways to remediate these issues.

The Skybox Appliance Setup Guide was streamlined and contained screen shots of the step-by-step process to get Skybox running. However, the guide does not mention the necessity to reboot the system after assigning an IP address.

The Skybox View Enterprise Suite does not offer no-cost customer support. The company does provide both eight hours a day five days a week and 24/7 service, though the price is calculated based on the licensing cost of the software. Several options for fee-based options are available.

The Skybox View Enterprise Suite is easy to install. After we connected the supplied flash drive, we simply ran the installer and waited for it to install the software into our test network. We configured basic logon information with the network configuration, which took us some time to troubleshoot. After we confirmed the problem was not caused by our test equipment we rebooted and were able to continue. From that point on we continued without any further issues.

Tenable Network Security

Nessus

Tenable Network Security Nessus is one of the most comprehensive and widely deployed vulnerability assessment tools. It is available as a software package for consumer versions of Microsoft Windows, Windows Server and Linux. It is also available as a preconfigured VM, an Amazon EC2 appliance, a preconfigured hardware appliance or a cloud service. Tenable has a wide variety of plugins which gives Nessus the ability to interface with basically any networked device. In addition, Nessus can be easily integrated with most major patch management systems, which gives administrators the ability to verify that updates are installing as they should be. Nessus can also be deployed with endpoint agents, which allow vulnerability scanning to occur offline and scan results can be collected after. This is valuable for mobile workforces where assets may not always be connected to the corporate network. The endpoint agents also allow Nessus to perform malware scanning. If a zero day has been identified within the organization, Nessus can be used to quickly check for other machines that have been infected organization-wide.

We received Nessus as an executable installation package for Windows. It took only minutes to install the software into our test network. After we connected the supplied flash drive, we simply ran the installer and waited for it to complete. After the installer finished, we were redirected to the web-based management interface automatically. The web interface was well-designed and very modern looking. We configured basic logon information and installed the provided license key, which downloaded all of the plugins for which we were licensed. Overall, setup was easy and straightforward.

Nessus has an easy-to-use, but very powerful interface. Policy creation is simple and only requires a few clicks to scan an entire corporate network. Nessus, overall, is straightforward to use and administer. Despite being simple, Nessus is an extremely powerful scanning tool with tons of functionality. Out of the box it comes with templates for virtually every major networking device on the market, as well as any firewall, virtualization host or cloud service one can think of. It also comes preloaded with the ability to scan every major operating system for vulnerabilities.

The initial purchase price is $1,500, and licensing follows a yearly renewal schedule. The yearly renewal cost is $1,200, which also includes access to Tenable support. This is the only support offering.

With its advanced scanning functionality and attractive pricepoint, we find this product to be of excellent value for the price. The software package is only $1,500 for the initial purchase, which makes it more accessible for most organizations than other options. Wide compatibility is also a valuable feature.
Tripwire IP360

The Tripwire IP360 appliance is a solution to advanced enterprise threat detection, vulnerability management and risk assessment. The solution can be purchased as a preconfigured hardware appliance or as a preconfigured VM. This appliance allows one to properly discover, analyze and respond to incidents on a network with its continuous network management and viewing capability. The comprehensive network view allows for a security team to properly and effectively develop both risk management strategies and policies to help mitigate network incidents.

The appliance was easily set up. We removed the device from the box and installed it into our server rack using the provided rack-mount hardware. After it was safely installed into our server rack, we connected our keyboard, monitor and mouse to the back of the server. Once powered on we configured the device using command-line. Setup went smoothly and the documentation was easily followed to complete the initial setup. The appliance is then accessed through the provided web interface that is well organized. The device’s license was preconfigured and allowed us to log in right into testing. This marked the end of the basic setup and configuration.

The product comes with an easy-to-use interface and allowed us to easily set up, manage and scan our test network. Within minutes of installation we were able to successfully run two scans and network audits. The solution comes with predefined scan capabilities and also allows custom scan creation and the ability to upload more scan policies. The report section of this product comes preconfigured with a Sarbanes-Oxley audit that we used to check compliance of our network hosts. The distinct audits section also allows users to upload custom audits, such as PCI, SCAP/CyberScope and JAVAs standards. Both the audits and scans can be exported in a variety of formats, including CSV, HTML, PDF and more.

Tripwire IP360 came with both a quick-start guide and a hardware setup guide. Both packs contained enough information for us to get the appliance properly installed and configured for first use. Seeing as the initial configuration is mainly command-line driven, the guide used highlighted text to identify required commands to get the device functional.

Tripwire provides clients with basic no-cost and fee-based support option. Free support is for one year and includes software upgrades with the purchase.

Overall, the Tripwire IP360 appliance can provide a security team with more than enough information to help discover, manage and remediate network vulnerabilities. The in-depth functionality of the user interface provides fluidity for its users who seek to quickly and effectively reduce network risk.

An innovative approach to Java security

Here’s the problem: Java is not secure. Here is the solution: sandbox Java apps. Well, it really is not quite that simple, but our First Look this month generated in us one of those “ah ha!” moments when we saw what it was and how it worked.

One of the major issues we face as security professionals is that application developers are usually tasked with application security and, as we all know, that often does not work as well as we’d like. Application security is difficult, and because new vulnerabilities appear regularly, it is very difficult to write truly secure code.

That said, we can, of course, write code that covers the big rocks. We can avoid buffer overflows and other common problems with some fairly straightforward coding practices. But there are subtleties—especially in Java—that get by even the most judicious coder. So one approach to protecting Java apps is to better protect the app, not just the code.

Before we hear anyone saying that we are encouraging sloppy coding, let us assure you that such really is not the case. However, the reality is that while attacks evolve once an app has been coded, it stays that way for some period of time. So even the best coding practice can become obsolete instantly with the emergence of new exploits. Before we get into the nuts and bolts of our product for this month, let’s take a quick look at an alternative.

The protection of the application from the outside is nothing new: We have application firewalls, for example, that attempt the same approach. However, these may tend toward false positives and certainly are not 100 percent reliable.

Waratek AppSecurity for Java claims to have that problem solved and its solution, as far as we can tell, is pretty solid. The application is containerized in what amounts to its own virtual machine. In fact, Waratek deploys its own hypervisor. AppSecurity for Java is based on a rule set that covers such things as language, I/O and other types of rules. The virtual containers, built on top of Oracle Hotspot, hold the security rules for the container. Those rules are crafted using the tools and the rules engine provided by Waratek. It all sounds pretty simple and, for the user, it is. What this really does, though, is let programmers concentrate on building their applications while the security experts worry about keeping the app safe.

The theory behind AppSecurity, at least in part, is what Gartner calls RASP: Runtime Application Self Protection. The idea behind RASP is that the security is built into the application’s Runtime environment. That means that everything the application does or interacts with is monitored. The application is containerized and sits on top of the Java Virtual Machine (JVM), which in turn sits on top of the operating system. The whole thing is neatly encapsulated in a controllable environment that satisfies the RASP paradigm.

We liked this tool both for its creative solution to a tough problem and its ease of deployment in the development environment. We see good things ahead for Waratek.

— Peter Stephenson, technology editor
Communicating security concepts

An ill-informed worker is a weak link that leaves a giant gap in your defenses, says SOHO Solutions VP Scott Aurnou.

Mistakes made by non-technical personnel can have a severe effect on organizational networks. Hackers frequently target them and more advanced attacks often begin with social engineering. Ignoring that weak link leaves a giant gap in an organization’s defenses.

Among the risks that can be mitigated with proper training are the failure to patch, clicking on sketchy sites, using public wi-fi, opening phishing email attachments and falling for other social engineering tricks, like baiting and pretexting. Nothing will stop every single attack. Someone will eventually fall victim to an especially well-crafted spear phishing email or a watering hole attack. But there’s a big difference between “once in a while” and a recurring problem. If the goal is to protect the network, an ill-informed workforce makes for a substantial attack surface. It’s not that people don’t care about protecting themselves. It’s that they don’t know how. Effectively communicating the nature of various threats, as well as what to do about them, is essential to mitigating the risk. Whether it’s awareness training, preparing for or responding to a security incident, or simply day-to-day communication, getting your message across clearly can only help.

Many non-tech-savvy people perceive security as dull, scary and pretty much incomprehensible. As a result, security professionals can find themselves fighting unnecessary uphill battles to get non-technical executives, employees, customers and potential customers on board with even simple security measures before there’s an emergency. The IT security field is becoming increasingly specialized (and effectively siloed) into narrower realms, like pentesting, mobile app security and zero-day research. As a result, it becomes more and more difficult for non-tech people to understand what’s going on without context. It’s essential to know your audience. Keep in mind that many of them don’t know what a byte is. They have no idea that memory and storage aren’t the same thing. And if the word “honeypot” makes them think of anything, it probably involves Winnie-the-Pooh. Security can be pretty intimidating to people who aren’t familiar with the underlying terminology. Imagine a doctor who keeps talking to you in detailed medical jargon and gets frustrated when you don’t understand it. It’s uncomfortable for you and you won’t learn much that way.

So, what do you do? Simple: tailor your message to their knowledge base. Two ways to accomplish this are analogies to familiar non-technical concepts and relevant pop culture references. One analogy I like to use is comparing overwriting to the tire tread. Another is explaining the difference between whistling and blacklisting as akin to the difference between an invite-only party and a club with a bouncer who throws people out once they’ve done something wrong.

A pop culture reference can be something like Q’s curious decision to plug the villain’s laptop into MI 6’s network in the recent James Bond film Skyfall as an example of baiting (let’s not get started on the plausibility of the subsequent hacking itself). And, the warehouse scene in Beverly Hills Cop is a perfect example of pretexting in action. Essential IT security concepts really shouldn’t be difficult to understand. If you use the listener’s own knowledge to help, these ideas won’t be difficult for them to absorb.

Scott Aurnou is an attorney, cybersecurity consultant and VP at SOHO Solutions.
YOUR ONE SHINING MOMENT

2015 SC Awards

Tuesday, April 21, 2015
InterContinental San Francisco

Visit awards.scmagazine.com
to view the finalists and book tickets.