2015 Cost of Failed Trust Report:

When Trust Online Breaks, Businesses Lose Customers

This is the second part of the Ponemon Institute’s 2015 Cost of Failed Trust Report, which reveals the damaging impacts on global business from unprotected cryptographic keys and digital certificates. This new report reveals that most companies lose customers, suffer costly outages, fail audits, and experience breaches due to unprotected and poorly managed keys and certificates.

Underwritten by Venafi
In March 2015, the Ponemon Institute and Venafi published research on the risks global business face from attacks on the Internet system of trust established by cryptographic keys and digital certificates. Consensus among the over 2,300 participants in Australia, France, Germany, UK, and US was that the system of trust was at the breaking point.

Analysis of previously unpublished data provides additional insights into the importance of securing keys and certificates in business today. Much of the world’s economy depends on the Internet, and keys and certificates are the foundation of online security. They secure communications and provide authorization and authentication. Global enterprises depend on the trust, privacy, and integrity established by keys and certificates.

There are numerous consequences when this foundation isn’t safeguarded. This second part of the 2015 Cost of Failed Trust Report, looks at how the failure to secure and manage keys and certificates is adversely impacting today’s businesses, and quantifies the direct financial impacts.

- **Unsecured keys and certificates are damaging businesses:** Nearly two-thirds of respondents (59%) admitted to losing customers because they failed to secure the online trust established by keys and certificates. In addition, business systems are failing with an average of over 2 certificate-related unplanned outages per organization over the last 2 years, with an average cost of $15 million per outage. Not surprisingly, businesses also failed one or more SSL/TLS and SSH audits during that same time period.

- **The risk continues—at great cost:** Our reliance on keys and certificates continues to grow with their increased use for SSL/TLS as well as mobile, WiFi, and VPN access, and the explosion of Internet of Things (IoT) devices. This increased reliance goes hand in hand with increased availability, compliance, and security risks. However, the amount of risk is not equal across these areas—security risk at $53 million over the next 2 years dwarfs availability and compliance risk, which totals $7.2 million.

- **Challenges must be addressed:** Over half (54%) admitted to a lack of visibility and a lack of policy enforcement and remediation for keys and certificates. Organizations must address these challenges which underlie the security, availability, and compliance risks caused by unsecure keys and certificates.
Global Demographics: All Suffer Losses

This report includes unpublished data from the survey conducted for the March 2015 Ponemon report, 2015 Cost of Failed Trust Report: Trust Online is at the Breaking Point. The 2015 research survey was completed by 2,394 IT security professionals around the globe: 646 U.S., 499 U.K., 574 German, 339 French, and 336 Australian respondents. The quantity and geographic breadth of the respondents shows that businesses around the globe are suffering the damaging impacts of unsecured keys and certificates.

Most respondents were from large enterprises with 59% from organizations with 5,000 or more employees. For the respondents’ roles, 42% were Administrators, 37% Managers to Supervisors, 17% Executive VP to Director, and 4% other. The largest verticals represented were financial services (17%), government (11%), professional services (8%), consumer products (7%), and retail (7%).

When Trust Online Breaks

We all have seen Global 2000 businesses in the headlines for breaches that leveraged keys and certificates. This has included Community Health Systems (CHS), that had data stolen on 4.5 million patients using the Heartbleed vulnerability; Sony Entertainment, which had SSH keys stolen; JPMorgan Chase, which had a certificate compromised and 90 of its servers breached; and Anthem, which had information on as many as 80 million people compromised.
NEARLY 2/3 OF BUSINESSES ADMIT TO LOSING CUSTOMERS
These businesses lost customers within the last 2 years because they failed to secure the online trust established by keys and certificates.

Businesses rely on keys and certificates to provide private communications and authorize and authenticate access to online services. This dependence on keys and certificates establishes online trust, giving customers the confidence to conduct online business. As a result, keys and certificates are at the foundation of security that supports much of the world’s economy.

When this trust is broken, businesses lose customers. Breaches can rack up millions in costs from incident response, settlements, legal fees, fines, and more. But one of the most damaging costs is customer churn—not only from those that were directly impacted by a breach, but also those that lose faith in the breached organization’s security.

In this study, nearly two-thirds (59%) of respondents admitted to losing customers because they failed to secure the online trust established by keys and certificates. With increased awareness around identity theft, phishing, and other online threats to privacy and finances, businesses will lose customers if they cannot ensure safe online access.

When Trust Online Breaks
In other Ponemon Institute research, lost business was one of three main contributors to the higher cost of data breaches in 2015—potentially resulting in the most costly impact following a breach. This loss of business included, “the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill.”

Share the research
Organizations are increasing their reliance on digital certificates to enable SSL/TLS and for mobile, WiFi, and VPN access. And the proliferation of connected Internet of Things devices means more even more certificates. However, when these digital certificates expire they block access to servers, websites, and potentially dozens of critical downstream services. If these certificates are not properly managed, the resulting expirations create outages which lower productivity and, ultimately, cause brand damage, and lost revenue, profits, and customers.

The threat of certificate-related outages is very real. The average organization has suffered more than 2 system failures due to certificate-related outages within the last 24 months. These outages are costing businesses millions. Security professionals estimated that the average cost of an unplanned certificate-related outage is $15 million.

**When Trust Online Breaks**

Gartner estimates that there are 4.9 billion Internet of Things devices connected to the Internet in 2015 and this will grow to 25 billion devices by 2020. We have seen hacks of cars including Jeep, Tesla, and any General Motors vehicle equipped with OnStar using the RemoteLink app. However, as our reliance on the Internet of Things expands, we will need to ensure that our access to medical devices, airlines, traffic light systems, hotel rooms, industrial systems, and other critical devices and systems remains secure and available.

**CRITICAL SYSTEMS FAILED**

Globally an average of over 2 business systems per organization stopped working over the last 2 years due to certificate-related outages.

**LOOSING $15 MILLION PER OUTAGE**

Security pros estimate this as the average impact per unplanned outage.
AUDITORS ARE CLAMPING DOWN

Over the last 2 years, every business has failed at least 1 SSL/TLS audit and at least 1 SSH audit.

Because keys and certificates are relied on so heavily for authentication, encryption, and assurance, standards—including regulatory, industry, and internal governance standards—dictate requirements for their proper usage. Keys and certificates are a great enabler of security, privacy, integrity, and access, but only when the right processes and technologies are applied.

Audits of key and certificate usage provide an opportunity for organizations to assess how they enforce issuance, renewal, replacement, and authorization, allowing them to close security gaps and stop outages. However, organizations are finding that these standards require more than most can deliver. On average, organizations failed at least one SSL/TLS audit and at least one SSH audit within the last 24 months.

When Trust Online Breaks

With vulnerabilities like Heartbleed, POODLE, and Shellshock eroding the trust established by keys and certificates and outages costing millions, audit findings for key and certificate usage has taken on new significance. Some well-known standards that address keys and certificates include the following:

- SANS Critical Security Controls
- ISO/IEC 27002–2013
- NIST 800–53
- PCI-DSS
- HITRUST
- And more…

Share the research
With unprotected keys and certificates, organizations are faced with security, availability, and compliance related risks. However, these risks are not equal. The security risk from unprotected keys and certificates dwarfs those for availability and compliance.

Security professionals estimate that, per organization, the combined risk for both key- and certificate-related availability and compliance issues is $7.2 million. This risk is the possible damage to an organization over the next two years (risk equals probability of occurrence times cost of total impact). Security risk, on the other hand, was estimated at $53 million—over 7 times as much. And this is up 51% from 2013 ($35 million).

**When Trust Online Breaks**

Of the key and certificate attack types, a cryptoapocalypse carries the greatest security risk over the next 2 years at $20 million.

Cryptoapocalypse: a discovered cryptographic weakness that becomes the ultimate weapon, allowing websites, payment transactions, stock trades, and governments to be spoofed or surveilled (term was coined by researchers presenting their findings at Black Hat 2013).\(^{11}\)

---

**SECURITY RISK DWARFS AVAILABILITY AND COMPLIANCE RISK**

Total risk per organization over the next 2 years:
- **$7.2M** Combined availability and compliance risk
- **$53M** Risk of attack using keys and certificates

---

**SECURITY RISK UP 51%**

From 2013 ($35 Million)
Why is trust online breaking and why are businesses failing? IT security teams lack the visibility and the policy enforcement to determine what’s trusted and what’s not. As was highlighted in the first 2015 Cost of Failed Trust Report, 54% of security professionals said they don’t know how many keys they have, where they are all located, or how they are used. This is up from 50% two years ago. However, most security analysts believe this number to be grossly underestimated.

Similarly, 54% said they lack policy enforcement and remediation for keys and certificates. With most security teams trying to manage keys and certificates with spreadsheets, it is impossible to conduct accurate tracking or to secure the entire key and certificate lifecycle. As the number of keys and certificates grows, the risks from unprotected keys and certificates will only get worse.

When Trust Online Breaks

With Google prioritizing search results for sites using HTTPS and organizations considering an Encrypt Everything approach, the drive to activate and expand encryption is gaining support from all types of businesses. With the average organization already using at least 23,922 keys and certificates, managing the deployment of even more will prove challenging for most organizations.
Unprotected keys and certificates are jeopardizing the digital trust which underpins the world’s economy. With a lack of visibility, policy enforcement, and remediation, unprotected keys and certificates are causing a loss of customers, system outages, and audit failures. Protecting keys and certificates must become a priority or businesses will continue to fail.

What is needed to secure keys and certificates and regain online trust? Organizations need to initiate processes and technologies that allow them to gain complete visibility into their key and certificate inventory and apply policies that comply with regulatory, industry, and internal governance standards—to avoid both outages and compromise. With this visibility, businesses must then be able to assess the trustworthiness of keys and certificates. When deemed untrustworthy, they must be able to remediate quickly to preserve their business and brand. Many of these processes should be automated, enabling keys and certificates to support dynamic technologies and innovation.

Biological systems have immune systems that identify what is self, good, and trusted. Similarly, the Internet uses keys and certificates for identification. However, there has not been an immune system for the cyber realm to indicate which keys and certificates should be trusted and which should not.

The insights from this study provide further evidence into how fragile the Internet system of trust is and how important it is for businesses to have an immune system for the cyber realm to secure keys and certificates.

**ACTION PLAN**

1. Know what’s being used: find all keys and certificates
2. Establish what should be trusted: enforce policy, automate security
3. Always know what’s trusted, what’s not: continuously monitor, check reputation for all
4. Remediate what’s not trusted: fix and replace vulnerable keys and certificates
About Ponemon Institute
Ponemon Institute conducts independent research on privacy, data protection and information security policy. Our goal is to enable organizations in both the private and public sectors to have a clearer understanding of the trends in practices, perceptions and potential threats that will affect the collection, management and safeguarding of personal and confidential information about individuals and organizations. Ponemon Institute research informs organizations on how to improve upon their data protection initiatives and enhance their brand and reputation as a trusted enterprise. You can learn more by visiting Ponemon.org.

References
13. Finley, Klint. WIRED. It’s Time to Encrypt the Entire Internet. April 17, 2014.

About Venafi
Venafi is the Immune System for the Internet™ that protects the foundation of all cybersecurity—keys and certificates—they can’t be misused by bad guys in attacks. Venafi constantly assesses which keys and certificates are trusted, protects those that should be trusted, and fixes or blocks those that are not.

Copyright © 2015 Venafi, Inc. All rights reserved. Venafi, Inc.
Part number: 1-0049-0915