2015 Cost of Failed Trust Report: Trust Online is at the Breaking Point

The Ponemon Institute's *2015 Cost of Failed Trust Report* reveals most organizations believe the trust established by cryptographic keys and digital certificates, which they require for their businesses to operate, is in jeopardy.

Underwritten by Venafi

Ponemon INSTITUTE

VENAFI

Executive Summary

The *2015 Cost of Failed Trust Report* presents research from Ponemon Institute, underwritten by Venafi, conducted with the help of 2,300 IT security professionals in Australia, France, Germany, the U.K., and the U.S.

The world's economy is built on the flow, sharing, and processing of data. Before the Internet could power the global economy, trusting data to be authentic, private, and unaltered was both a core requirement and an insurmountable barrier. The solution was the use of cryptographic keys and digital certificates to establish authenticity and privacy online. Now the trust behind trillions of dollars in the world's economy comes down to just a few kilobytes of cryptographic keys and their associated digital certificates.

After weathering a rising tide of attacks and vulnerabilities, the *2015 Cost of Failed Trust Report* research shows the digital trust that underpins most of the world's economy is nearing its breaking point, and there is no replacement in sight. This research found that thousands of IT security professionals believe that, over the next two years, the risk facing every Global 5000 from attacks on keys and certificates is at least $53M. This is up 51% from the risk estimated in 2013. And for four years running, all of the organizations surveyed have responded to multiple attacks on keys and certificates.

Security professionals rank a *Cryptoapocalypse*–like event, a scenario where the standard algorithms of trust like RSA and SHA are compromised and exploited overnight, as the most alarming threat.[1] But lurking close behind in second place is the misuse of certificates used for enterprise mobility with applications like WiFi, VPN, and MDM/EMM.

The research includes these important key findings:

- **At the same time risk increases, the number of keys and certificates grows:** Over the last two years, the number of keys and certificates deployed on infrastructure such as web servers, network appliances, and cloud services has grown over 34% to almost 24,000 per enterprise—and this doesn't include those used beyond the firewall with mobile devices, mobile applications, or numerous devices that are part of the Internet of Things.
- **Organizations are even more uncertain about what should be trusted:** Also up from 2013, 54% of organizations admit to not knowing where all keys and certificates are located, which means they don't know how they're being used or what should be trusted.
- **Trust required to operate as a business is threatened:** Now 50% of security professionals, up from 45% two years ago, believe the trust their business requires to operate—in communications, in their data center, and out to the cloud, mobile devices, and Internet of Things (IoT)—is in jeopardy.

Global Demographics: 100% Attacked

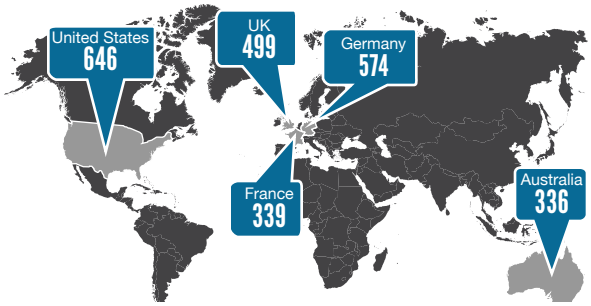
Over the last two years, and now for four years running, all respondents involved in this research have responded to attacks using keys and certificates. This is the only publicly available research to track the breadth and scope of these attacks.

The 2015 research survey was completed by 2,371 IT security professionals. 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%).

Trust is at the breaking point: Over the past two years a steady stream of incidents has made it clear that keys and certificates are under attack. In one example from 2014, an SSL/TLS certificate representing a top 5 global bank was found in the treasure trove of Russian cybercriminals' weapons stash. The certificate was used to impersonate the bank, steal other user credentials, and help to execute the theft of 80M customer records.[2]

2,394 RESPONDENTS

In Global 5,000 Organizations

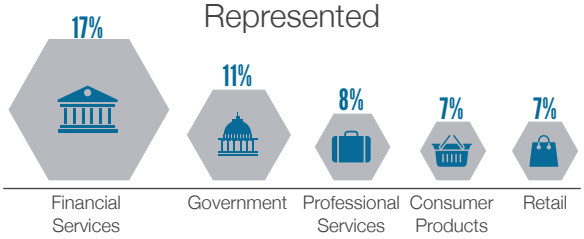


59% OF COMPANIES

Have 5,000 or more employees

TOP 5 INDUSTRIES

Represented



Types of Attacks Analyzed

This research examined six of the most common threats. The blueprint for attacks that use keys and certificates goes back to Stuxnet.[3] In that attack, a compromised code-signing certificate from Taiwan was used to gain trusted status for malicious code inside of Iranian nuclear facilities. Today, a range of attacks are now in the arsenal of common cybercriminals.

	Description of Attack Type	Example of Real-world Attack
Server Certificate Misuse	To impersonate public websites and decrypt encrypted traffic, attackers steal keys and certificates.	The theft of data on 4.5M healthcare patients in 2014 started with the exploit of Heartbleed to steal an SSL/TLS key and certificate that encrypted sensitive data.[4]
Code-signing Certificate Isuse	Attackers digitally sign malicious code to have it trusted and run.	The $1B theft by Carbanak operators was enabled by signed malware that looked like trusted software.[5]
SSH Key Misuse	Bad guys seeking to gain access to the most sensitive systems and data compromise SSH credentials.	APT operators like The Mask stole SSH keys and used their privileged access to compromise networks for over seven years.[6]
Man-in-the-middle (MITM) Attack	Cybercriminals compromise Certificate Authorities (CAs) or forge new certificates to trick users and monitor communications.	APT operators like Dark Hotel used a malicious CA and website certificates to get in and target executive communications.[7]
Weak Cryptographic Exploit	Adversaries target weak cryptography to create trusted keys and certificates.	As part of the Flame malware, Microsoft's software update service was spoofed by exploiting MD5-based signatures.[8]
Enterprise Mobility Certificate Misuse	Misuse of these credentials provides access to WiFi, VPN, or data protected by MDM/EMM systems.	An emerging threat that security professionals believe needs to be watched closely.

Attacks and Uncertainty Grow

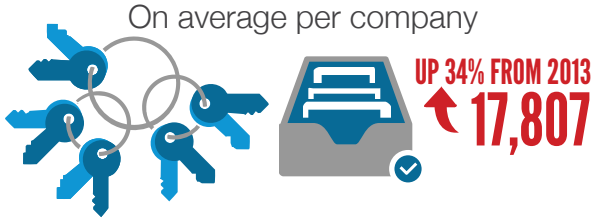
Over the last two years, the average number of SSL/TLS and SSH keys and certificates has grown 34% to at least 23,922. This growth is driven from an increasing number of needs: from more focus on privacy following Edward Snowden's NSA revelations (the BBC declared 2014 as the "Year of Encryption"[9]) to Google ranking sites with SSL/TLS and digital certificates more highly in its search results algorithm.[10]

As the number of keys and certificates grows, IT security teams are unable to keep up with what's trusted and what's not. Now 54% of security professionals (up from 50% two years ago) said they don't know where and how many keys and certificates are in use. However, most security analysts believe this number to be grossly underestimated. Accurate tracking is impossible when most security teams are trying to manage this with spreadsheets.

Trust is at the breaking point: A viscous cycle is at play. We need more keys and certificates to protect privacy and businesses. The importance and number of keys and certificates make them a target to exploit. More attacks drive more use. Now cybersecurity experts at Intel predict that the next large-scale hacker marketplace will be in the sale of stolen digital certificates.[11] In 2013, the price was almost $500.[12] In 2014, the price grew to almost $1000.[13]

23,922 KEYS & CERTIFICATES

On average per company



54% ARE UNAWARE

Most organizations do not know where all keys and certificates are located

$1000 PRICE TAG

For a stolen certificate in the underground marketplace

Heartbleed Takes its Toll

60% OF IT SECURITY TEAMS

Believe their organization needs to better respond to vulnerabilities involving keys and certificates

58% OF SECURITY TEAMS

Need to better secure and protect their keys and certifiates

In April 2014, the security of all SSL/TLS keys and certificates became uncertain with the discovery of the Heartbleed vulnerability. Experts from Bruce Schneier to Gartner implored enterprises to consider all keys and certificates compromised and replace them all.[5, 6]

Security teams scrambled to replace keys and certificates. For many, their first attempts took weeks and research shows most did not complete remediation and moved on.[16]

As a result, 60% of IT security teams believe their organization needs to better respond to vulnerabilities involving keys and certificates. Inline with this thinking, 58% of security teams agree that keys and certificates need to be better secured to deal with the rise in attacks.

Trust is at the breaking point:
In August 2014, the details of a breach that leaked data on 4.5M patients from a Fortune 500 healthcare operator became headline news. APT 18, a known Chinese cyberespionage operator, began their attack by using Heartbleed to compromise a key and certificate used with an SSL VPN. The key and certificate were not replaced following Heartbleed, leaving the door open to attackers for months.[4]

Threat of a Cryptoapocalyse

The steady stream of vulnerabilities and resulting attacks involving keys and certificates has weighed heavily on security professionals. The most alarming threat to security professionals in 2015 is now a cryptographic exploit leading to a meltdown in trust. A team of researchers presenting their findings at Black Hat 2013 termed this event a Cryptoapocalypse: where in a matter of days a cryptographic weakness discovered by a researcher becomes the ultimate weapon, allowing websites, payment transactions, stock trades, and even governments themselves to be spoofed or surveilled.[1] The resulting chaos and inability to trust much of the digital world could leave behind a global recession and worse.

Trust is at the breaking point: The idea of a Cryptoapocapyse is far from science fiction. Heartbleed was just a taste of what this could look like. Could a website be trusted? How many keys were compromised? Could an organization be trusted online? The era of cloud computing, parallel processing, and GPUs are being used to test these attacks. The cost to compromise a MD5–signed digital certificate is now $0.65[17] in Amazon AWS, down from $200,000 in less than two years.[18]

2015

MOST ALARMING THREATS (IN ORDER OF CONCERN)

1. WEAK CRYPTOGRAPHIC EXPLOIT
2. MOBILE CERTIFICATE MISUSE
3. CODE-SIGNING CERTIFICATE MISUSE
4. MALICIOUS MITM CERTIFICATES
5. SSH KEY MISUSE
6. SERVER CERTIFICATE MISUSE

MITM and Weak Crypto Exploits Hit Everyone

	Most Frequent Attacks Over the Last Two Years*	Most Expected Attacks Over the Next Two Years**
1	MITM attacks (1.4)	Weak cryptographic exploit (18%)
2	Weak cryptographic exploit (1.2)	Enterprise mobile certificate misuse (9%)
3	Enterprise mobility certificate misuse (0.4)	Code-signing certificate misuse (7%)
4	Code-signing certificate misuse (0.4)	MITM attacks (7%)
5	SSH key misuse (0.3)	SSH key misuse (4%)
6	Server certificate misuse (0.3)	Server certificate misuse (3%)

* The number noted in "()" represents the number of times a company responded to the type of attack over the last two years.

** The percentage note in "()" represents the likelihood a particular type of attack will occur over the next two years.

The malicious use of certificates to execute MITM attacks and weak cryptographic exploits that allow communications to be spoofed were the two most common attacks over the last two years. One or more of these incidents were responded to by every organization in the survey. Over the next two years, organizations expect they will respond most often to weak cryptographic exploits and misuse of enterprise mobility certificates.

Trust is at the breaking point:

MITM attacks are now a common attack tool. From organized Chinese government efforts that occur on an almost daily basis to APT operators targeting executives in the Dark Hotel campaign,[7] MITM attacks with valid or forged certificates are powerful attacks that undermine multiple layers of security. By getting in between users and what they believe are trusted websites, attackers can capture user credentials and intellectual property en masse.

Facebook along with Carnegie Mellon[t] found over 6,000 forged certificates used for MITM operations with many of them actively in use by attackers.[19] The power of this type of attack was demonstrated when Lenovo included adware that created a fake CA, which allowed MITM attacks to be conducted on any website and go virtually undetected.[20]

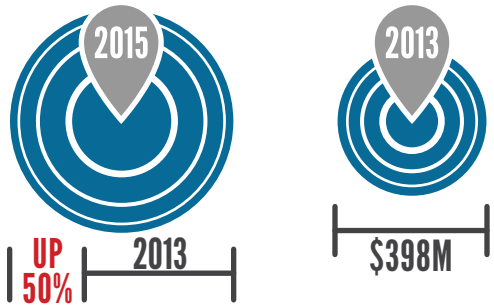
Risks and Impact Surge

As a result of increased attacks and the expectation that more will occur, security professionals estimate that the average risk facing organizations from attacks on keys and certificates is now $53M, up 51% from 2013. Risk is the possible damage of attacks occurring in any given organization over the next two years (risk equals probability of attack times total impact). The total possible impact of all attacks now reaches $597M, up 50% from 2013.

Trust is at the breaking point:

Greatest Risk
- $22M Weak cryptographic exploit
- $11M Mobility certificate misuse
- $8.4M Code-signing certificate misuse
- $6.5M MITM attacks
- $3.1M SSH key misuse
- $1.9M Server certificate misuse

Largest Impact
- $126M Mobility certificate misuse
- $114M Weak cryptographic exploit
- $102M Code-signing certificate misuse
- $93M SSH key theft
- $90M MITM attacks
- $73M Server certificate misuse



Uncertainty Over Mobile Looms Large

$126M

TOTAL IMPACT OF AN EXPLOITED ENTERPRISE MOBILITY CERTIFICATE—WIFI, VPN, OR MDM/EMM

$11M

TWO-YEAR RISK OF AN EXPLOITED ENTERPRISE MOBILITY CERTIFICATE (PROBABILITY OF ATTACK TIMES TOTAL IMPACT)

77%

IT SECURITY PROFESSIONALS THAT DO NOT HAVE VISIBILITY INTO MOBILE CERTIFICATE USAGE

Not only did security professionals find the misuse of enterprise mobility certificates the second most alarming threat over the next two years—if exploited, it's likely to cost the most! Respondents place the total impact of an exploited enterprise mobility certificate—one that's used with WiFi, VPN, or MDM/EMM—at up to $126M and a two-year risk of almost $11M. With an expected increase of mobile devices across enterprises, security professionals are clearly uneasy with the increased risk this creates.

Trust is at the breaking point: Recent Forrester research found 77% of IT security professionals do not have complete visibility into how their organizations are using mobile certificates for WiFi, VPN, and MDM/EMM. Add to this that 62% could not detect anomalous mobile certificate usage and the reasons why security teams are so alarmed by the misuse of enterprise mobility certificates becomes clear.[21]

Conclusion: The Breaking Point

The result of more attacks, vulnerabilities, and risk over the last two years is that IT security professionals believe the trust they need in digital systems and data for their business to operate is now in jeopardy.

Up from 45% two years ago, half of respondents agreed the trust established by keys and certificates is in jeopardy. Half believe the way we create trust is broken. Half of IT security professionals now agrees with Gartner's 2012 research finding that "certificates can no longer be blindly trusted."[22]

The over 2,300 IT security professionals that participated in this research have become figurative "canaries in the coal mine"—alerting the world and their senior management teams that the security technology we've relied on for over 20 years and built into every digital device and transaction is near the breaking point. With keys and certificates so broadly deployed, and so integral to the future, they must be better secured and protected. With no replacement in sight, failure is not an option. As security technology has adapted to today's changing threatscape, new ways of ensuring the trust established by keys and certificates remains safe must be developed as a top IT security priority.

Trust is in Jeopardy

HALF OF IT SECURITY PROFESSIONALS BELIEVE

- TRUST ESTABLISHED BY KEYS AND CERTIFICATES IS IN JEOPARDY
- THE WAY WE CREATE TRUST IS BROKEN
- GARTNER IS RIGHT, "CERTIFICATES CAN NO LONGER BE BLINDLY TRUSTED."

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.

About Venafi

Venafi is the leading cybersecurity company in Next Generation Trust Protection. Venafi delivered the first trust protection platform to manage, secure, and protect cryptographic keys and digital certificates that every business and government depends on for secure communications, commerce, computing, and mobility. For more information, visit Venafi.com.

Part number: 1-0039-0315

References

1. Stamos, Alex, et al. Blackhat USA 2013. *Preparing for the Cryptopocalypse.* July 2013.
2. Perlroth, Nicole and Gelles, David. NYTimes.com. *Russian Hackers Amass Over a Billion Internet Passwords.* August 5, 2014.
3. GReAT. Securelist. *Stuxnet: Zero Victims.* November 11, 2014.
4. Davek. TrustedSec. *CHS Hacked via Heartbleed Vulnerability.* August 19, 2014.
5. Fagerland, Snorre. Blue Coat Labs Blog. *Carbanak/Anunak in the BlueCoat Malware Analysis Appliance.* February 18, 2015.
6. Kaspersky Lab. Virus News. *Kaspersky Lab Uncovers "The Mask."* February 11, 2014.
7. Drozhzhin, Alex. Kaspersky Lab Daily Blog. *Darkhotel: A Spy Campaign in Luxury Asian Hotels.* November 10, 2014.
8. Lemos, Robert. eWeek. *Flame Exploited Long-Known Flaw in MD5 Certificate Algorithm.* June 13, 2012.
9. Rubens, Paul. BBC News. *2014: The Year of Encryption.* January 9, 2014.
10. Ait Bahajji, Zineb and Illyes, Gary. Google Online Security Blog. *HTTPS as a Ranking Signal.* August 6, 2014.
11. Rosenquist, Matthew. Intel IT Expert Blog. *Stealing Certificates to Sign Malware Will be the Next Big Market for Hackers.* December 23, 2014.
12. Monsted, Jonas. CSIS Blog. *Digitally Signed Malware 2013.* December 3, 2013.
13. Koyfman, Tanya. SenseCy. *Malware is Coming to the Trusted Software Near to You – Trade in Code Signing Certificates is on the Rise on the Russian Underground.* October 13, 2014.
14. Schneier, Bruce. Schneier on Security. *Heartbleed.* April 9, 2014
15. Heidt, Erik T. Gartner Blog Network. *Heartbleed Exploit in OpenSSL – How Should You Respond?* April 9, 2014.
16. Ventsias, Tom. University of Maryland, UMD Right Now. *UMD Cyber Experts Discover Lapses in Heartbleed Bug Fix.* November 7, 2014.
17. Goodin, Dan. Ars Technica. *Crypto Attack that Hijacked Windows Update Goes Mainstream in Amazon Cloud.* November 5, 2014.
18. Goodin, Dan. Ars Technica. *Flame's Crypto Attack May Have Needed $200,000 Worth of Compute Power.* June 11, 2012.
19. Huang, Lin-Shung, et al. Carnegie Mellon University and Facebook. IEEE Symposium on Security and Privacy (IEEE S&P). *Analyzing Forged SSL Certificates in the Wild.* 2014.
20. Peters, Sara. InformationWeek Dark Reading. *Superfish Compromises All SSL Connections on Lenovo Gear.* February 19, 2015.
21. Forrester. *IT Security's Responsibility: Protecting Mobile Certificates.* June 2014.
22. MacDonald, Neil and Valdes, Ray. Gartner. *Maverick Research: Living in a World Without Trust: When IT's Supply Chain Integrity and Online Infrastructure Get Pwned.* Gartner Doc: G00238476. October 5, 2012.