2013 Annual Cost of Failed Trust Report: Threats & Attacks

The Ponemon Institute's First Annual Cost of Trust Report reveals that failed key and certificate management threatens every global enterprise with potential cost exposure of almost U.S. $400M.

Underwritten by Venafi

VENAFI

Table of Contents

Ponemon INSTITUTE

Executive Summary

The *First Annual Cost of Failed Trust Report: Threats & Attacks* presents research from Ponemon Institute, underwritten by Venafi. The report provides the first extensive examination of how failure to control trust in the face of new and evolving threats is placing all global enterprises at risk. Based on survey participant expectations, organizations are projected to lose $35 million over the next 24 months. This estimate is based on a total possible cost exposure of $398 million (USD) per organization. These and other conclusions are based on new primary research conducted in Australia, France, Germany, the U.K. and the U.S. with 2,342 respondents from mostly Global 2000 enterprises.

Every business and government relies on cryptographic keys and certificates to provide trust for critical electronic communications. These technologies underpin the modern world of card payments, online shopping, smartphones and cloud computing. But, unlike before—when trust could be measured in terms of locks, safes and security cameras—executives, even those in IT security, little understand how truly fragile trust is today. A few kilobytes of cryptographic data is all that stands in the way of millions lost in sales, grounded airplanes and closed borders.

Unfortunately, criminals now understand how fragile our ability to control trust has become. The pervasiveness of cryptographic keys and certificates, as well as the protocols that depend upon them, makes exploiting trust very attractive. Businesses' inability to detect attacks on trust, or take action if they do, makes the target all that more appealing. To date, the global financial impact of the attacks, the extent of the challenges

$398M

LOSSES FACING EVERY GLOBAL 2000 ORGANIZATION FROM ATTACKS ON TRUST
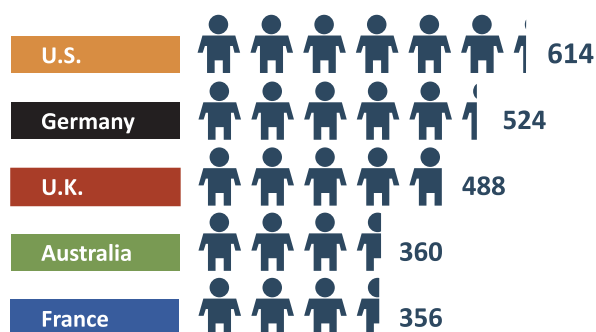
18%

OF ENTERPRISES EXPECT TO FALL PREY TO ATTACKS DUE TO USING WEAK, LEGACY CRYPTOGRAPHY OVER THE NEXT 2 YEARS
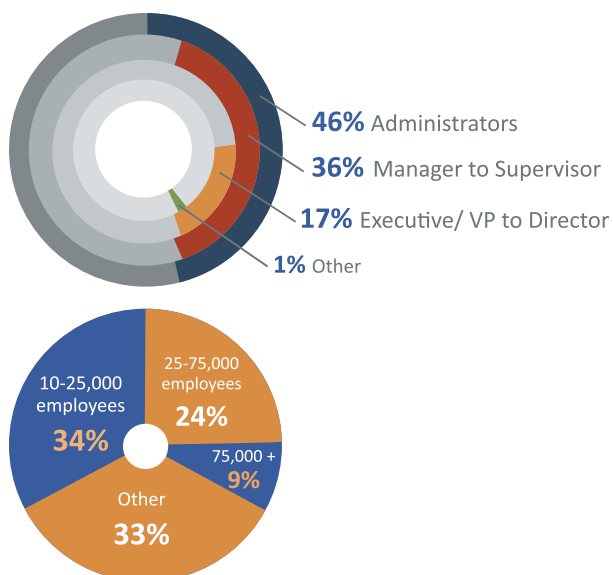
$125M

WITH EACH ATTACK COSTING AN ORGANIZATION UP TO $125M THE MOST EXPENSIVE KEY MANAGEMENT FAILURE WHICH IS EASILY PREVENTABLE

2,342 survey respondents from within the Global 2000

U.S.	614
Germany	524
U.K.	488
Australia	360
France	356

The Ponemon Institute vetted respondents

46% Administrators
36% Manager to Supervisor
17% Executive/ VP to Director
1% Other

25-75,000 employees **24%**
10-25,000 employees **34%**
75,000 + **9%**
Other **33%**

for closing vulnerabilities and even the industry's recognition that attacks are occurring have remained largely unquantified.

Critically important findings of this research include:

- **$400M is at risk in every enterprise**— Every Global 2000 organization faces an average of $35 million in potential losses from evolving attacks that exploit shortfalls in controlling trust from failures in cryptographic key and digital certificate management. This estimate is based on a total possible cost exposure of almost $400 million.

- **Exploits of weak cryptography are most likely and costly**—Eighteen percent of enterprises expect to fall prey to attacks due to using weak, legacy cryptography over the next 2 years. With each attack representing a possible total cost exposure of $125M over two years, this easily preventable problem is the single most expensive key management failure identified by this research.

- **Attacks on trust providers take their toll**— Man-in-the-middle and phishing attacks that use compromised Certificate Authorities (CAs) and certificates to impersonate trusted identities with a possible total cost exposure of $73M over two years, per organization.

- **No enterprise is safe**—All global enterprises surveyed have been impacted by their inability to control trust.

In addition to revealing the financial impact of failing to control trust, the research also reveals the extent of the challenge facing enterprises in managing their keys and certificates, as highlighted in these findings:

- **The vast problem cannot be handled manually**—Enterprises estimate they have on average 17,807 keys and certificates deployed on infrastructure such as web servers, databases, network devices and cloud services; 45 percent believe that failing to manage keys and certificates directly leads to the erosion of the trust on which their business depends.

- **Most cannot even describe their control over trust**—Fifty-one percent of Global 2000 organizations do not know exactly how many keys and certificates they have in their infrastructure. This represents systemic and unquantified risk.

- **Technology critical to cloud computing is in clear and present danger**—Organizations surveyed believe attacks on Secure Shell (SSH) keys, the basic technology used to establish trust and connections with cloud services from Amazon and Microsoft, present the most alarming threat arising from failure to control trust. The inability to detect and take action in the event of an attack on SSH keys compounds the risk and potential costs.

- **Establishing control over trust will change the outcome**—Already 59 percent of enterprises believe that, if they establish proper key and certificate management before using new encryption and authentication technologies, they will regain control over trust and end the present risks of security breaches, unplanned outages, and failed audit and compliance.

17,807

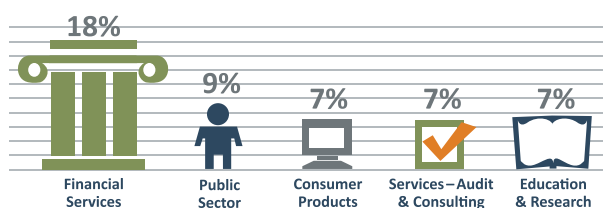## AVERAGE NUMBER OF SERVER KEYS AND CERTIFICATES IN A GLOBAL 2000 ORGANIZATION

51%

DON'T KNOW HOW MANY KEYS AND CERTIFICATES ARE IN USE BY THEIR ORGANIZATION

45%

"FAILING TO MANAGE KEYS AND CERTIFICATES MEANS LOSING CONTROL OVER THE TRUST MY ORGANIZATION RELIES UPON TO OPERATE."

Global Demographics

18%
9%
7% 7% 7%

Financial Services | Public Sector | Consumer Products | Services – Audit & Consulting | Education & Research

To evaluate the attacks and exploits that arise from failure to manage cryptographic keys and digital certificates, Ponemon Institute surveyed 2,342 respondents from within the Global 2000. The number of respondents varied from country to country:

U.S.—614   Germany—524   U.K.—488
Australia—360   France—356

Among these five nations, 16 unique vertical industries were identified. The top 5 verticals represented in this survey are:

Financial services—**18%**
Public sector—**9%**
Consumer products—**7%**
Services, including audit and consulting—**7%**
Education and research—**7%**

Ponemon Institute vetted respondents from the Global 2000. Of those individuals surveyed:

● Seventeen percent were at the executive/vice president level, 20 percent at the manager level and 16 percent at the supervisor level.

● Sixty–seven percent of the respondents came from companies with 10,000 or more employees, including 34 percent with 25,000 or more employees.

All data related to monetary values was collected in local currency (dollars, euros or pounds) and converted to a common U.S. dollar value.

Ponemon INSTITUTE

Current State of Controlling Trust

This research reveals that German enterprises are the most aware of the critical impact that cryptographic keys and digital certificates have on trust and that, as a whole, organizations based there are the most prepared to handle associated challenges. Fifty–four percent of German organizations are proactively adding layers of encryption technologies to comply with regulations and policies; only 32 percent of organizations in France and 39 percent of organizations in the U.S. are doing the same. German organizations are also the least concerned with losing control of cryptographic keys and certificates and the most aware of the number of keys and certificates in their infrastructure.

Enterprises taking proactive steps to add encryption layers in order to improve trust varied significantly:

Germany—52%   Australia—45%   U.K.—41%
U.S.—39%   France—32%

Not knowing how many cryptographic keys and certificates exist in its infrastructure essentially means an enterprise has lost its control over trust. A shocking number of enterprises do not know exactly how many keys and certificates they have deployed:

U.K.—61%   France—59%   U.S.—54%
Australia—47%   Germany—34%

Unable to discover where keys and certificates are deployed, how they are being used, and who is using them, an enterprise finds itself defenseless against direct or indirect attacks on trust.

The Cost of Attacks on Trust

1 OR MORE

TRUST EXPLOITS AND ATTACKS FROM KEY & CERTIFICATE MANAGEMENT FAILURES IN EVERY ORGANIZATION OVER LAST 2 YEARS

1 OUT 5

EXPECT A SUCCESSFUL TRUST EXPLOIT FROM KEY & CERTIFICATE MANAGEMENT FAILURES IN THEIR ORGANIZATION OVER NEXT 2 YEARS

#1

MOST ALARMING KEY & CERTIFICATE MANAGEMENT THREAT

Criminals are increasingly exploiting the trust established by cryptographic keys and certificates to facilitate attacks on business and governments. These attacks may be indirect such as when CAs such as DigiNotar and DigiCert were infiltrated, compromised and used to issue fraudulent certificates. The attacks may also be direct—for example, malware like Flame uses weaknesses in legacy cryptographic methods to infiltrate networks. Often, the attacks are nearly impossible to detect because of the unquestioning trust put in the complex cryptographic systems that enable activities from online banking to video streaming to software updates.

The research sought for the first time to evaluate the costs of attacks on trust, enabling enterprises to estimate the true financial impact of failing to manage trust. Respondents evaluated four cost categories for each type of attack:

- Incidence response
- Lost productivity
- Revenue loss
- Brand and reputation damage

The results show that businesses and governments now face a global average cost of $398M per organization from new and evolving attacks on trust. The high cost makes sense given that attacks on cryptographic keys and certificates are difficult to detect and also target the most critical IT and business processes. The costs are also in line with other major breaches such as TJX, which cost at least $256M.[1] However, most risk management professionals and auditors, and even many IT security professionals, are unaware of the potential losses in their organization if they fail to control trust in the face of new threats.

The report now breaks down the costs for each type of attack.

CA compromises used for man–in–the–middle and phishing attacks with a potential total cost exposure of $73,250,825.

U.S.—$78,357,191   U.K.—$62,558, 326
Australia—$66,324,265   Germany—$88,856,053
France—$63,135,809

Previously thought impossible, successful compromises of CAs are now commonplace. Whether infiltrating networks or using misleading information, criminals are gaining valid digital certificates that can be used to execute man–in–the–middle, phishing and other attacks that exploit a browser or application's trust of the attacker's certificate. Due to the alarming rise in these attacks, the U.S. National Institutes of Standards (NIST) published guidelines for all organizations to prepare and respond to CA compromises.
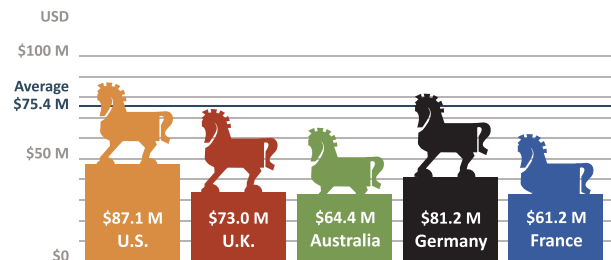
SSH key theft and compromise with an average potential cost exposure of $75,418,706.

U.S.—$87,118,657   U.K.—$72,966,849
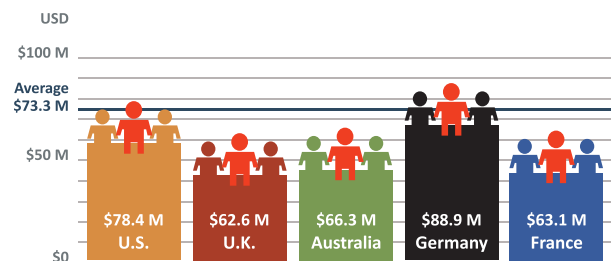Australia—$64,362,043   Germany—$81,229,309
France—$61,228,757

SSH

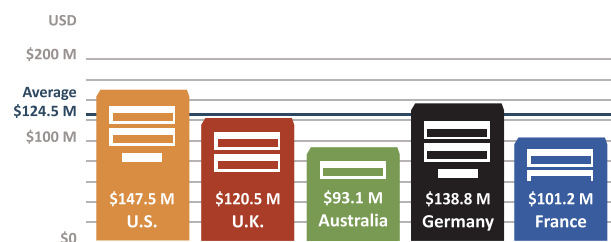## CRITICAL FOR ESTABLISHING TRUST AND CONTROL IN THE CLOUD
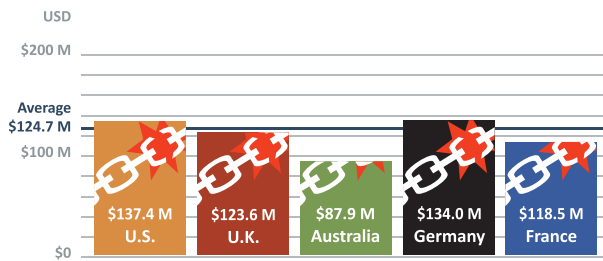
SSH key theft by Trojan (Global impact)

USD
$100 M
Average $75.4 M
$50 M
$0

| $87.1 M U.S. | $73.0 M U.K. | $64.4 M Australia | $81.2 M Germany | $61.2 M France |

Man-in-the-middle and Phishing attacks (Global impact)

USD
$100 M
Average $73.3 M
$50 M
$0

| $78.4 M U.S. | $62.6 M U.K. | $66.3 M Australia | $88.9 M Germany | $63.1 M France |

Server cryptographic key theft (Global impact)

USD
$200 M
Average $124.5 M
$100 M
$0

| $147.5 M U.S. | $120.5 M U.K. | $93.1 M Australia | $138.8 M Germany | $101.2 M France |

Ponemon
INSTITUTE

Weak cryptographic exploits (Global impact)

USD

$200 M

Average
$124.7 M

$100 M

| $137.4 M U.S. | $123.6 M U.K. | $87.9 M Australia | $134.0 M Germany | $118.5 M France |

$0

Trust-based attacks, broken down by geography

USD

$500 M

$400 M

$300 M

| $450.4 M U.S. | $379.6 M U.K. | $311.7 M Australia | $448.8 M Germany | $344.0 M France |

$200 M
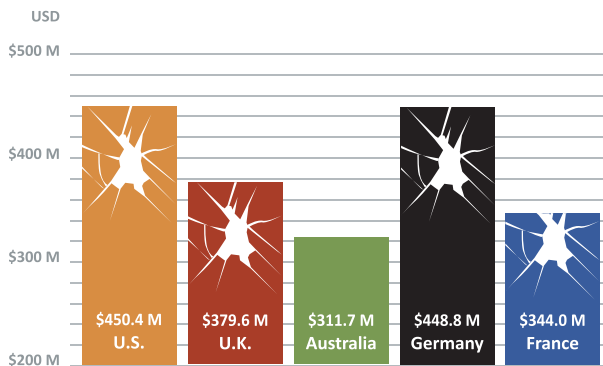
Not well known outside the domain of the system administrator, SSH is used extensively to establish secure connections between computers and provides root access to the systems. Organizations use SSH to maintain control and ownership of cloud systems such as Amazon Web Services and Microsoft Azure. Management of SSH is typically performed by system administrators and until recently infrequently audited. If a criminal were to obtain keys used by a trusted administrator or system, all connected systems and data, even if encrypted, could be compromised.

Server cryptographic key theft with an average potential cost exposure of $124,489,384.

U.S.—$147,465,880   U.K.—$120,462,575
Australia—$93,080,956   Germany—$138,745,327
France—$101,159,146

It is not surprising that the theft of server cryptographic keys topped the list of estimated costs. With these keys, an attacker can impersonate a web site or authenticate to an encrypted database full of credit card numbers. These attacks are hard to detect since, cryptographically, the attacker and legitimate system are identical.

Weak cryptographic exploits with an average potential cost exposure of $124,617,926.

U.S.—$137,409,392   U.K.—$123,575,122
Australia—$87,936,513   Germany—$139,957,136
France—$118,501,328

A growing range of devastating malware is now using weaknesses in legacy cryptography to execute attacks. Malware such as Stuxnet, Duqu and Flame target weaknesses in cryptographic methods (such as the MD5 hash algorithm) that may be deprecated but are still widely in use. Because these attacks appear to be cryptographically valid, malware can spread quickly and reach highly sensitive systems and data.

Total estimated costs across all five geographies show the maximum average potential cost exposure for losing control over trust in the U.S. and Germany.

U.S.—$450,351,119   U.K.—$379,562,872
Australia—$311,703,776 Germany—$448,787,825
France—$344,025,040

Ponemon
INSTITUTE

The Risk of Attacks on Trust

In all cases, enterprises have experienced one type of these attacks over the last 24 months, and many expect to encounter the same or new attacks in the next 24 months.

	Average incidents over last 24 months per respondent's enterprise	Average likelihood of attack in respondent's enterprise over next 24 months
Man-in-the-middle/phishing attack via CA compromise	1.1	7%
SSH key theft	0.3	3%
Server key theft	0.4	5%
Weak cryptographic exploit	1.3	18%

Clearly, organizations underestimate the likelihood of future attacks at about 18 percent, given that all organizations have experienced one type of attack before. The research also shows that, even if the likelihood of an attack is low today, the result of just one attack can be all too serious.

Most Alarming New Threat to Trust: Attacks on SSH

Respondents were asked to identify the most alarming attack on trust due to failed key and certificate management. Overwhelmingly across all five geographies, SSH key theft alarmed respondents the most. While enterprises have experienced other attacks, respondents judged this attack the most severe.

This new finding has significant implications for cloud computing since Infrastructure as a Service (IaaS) providers rely on SSH to give customers control and ownership over systems and data running in the cloud. Without SSH, enterprises would lose direct and immediate control over their data and business processes in the cloud.

To date, internal and external auditors and risk management professionals have paid little attention to SSH. However, given the technology's importance to the cloud and its frequent self-management by system administrators, it is likely that SSH will come under the increasing scrutiny of audit and compliance teams. The research results appear to show that failing to address this new threat will significantly degrade the trust that organizations have in their infrastructure, especially its security, as they move to the cloud.

Ponemon
INSTITUTE

Conclusion:
Regaining Control over Trust

The research clearly reveals that enterprises are having difficulties retaining control over trust. Fifty-one percent of enterprises admit that failure to manage keys and certificates means losing control over trust. Further, 40 percent openly admitted that their own inability to control keys and certificates is already placing sensitive and valuable data at risk. Given that all organizations have experienced attacks that exploit their inability to control trust, we expect these numbers to increase in the future.

In 2010, Forrester Research stated that the future opportunity for IT is to "Own nothing, control everything."[2] Moving to cloud computing and Bring Your Own Device (BYOD) environments certainly offer the opportunity for IT to own less. Controlling everything, however, requires IT to regain control over the cryptographic keys and certificates that create and manage trust for cloud and mobile computing—as well as in the current IT data center environment. CEOs and CIOs do not need to become experts in these technologies. However, they must understand that, unless businesses and governments can regain their control over trust by managing their keys and certificates properly, the future will be "Own Nothing. Control Nothing." Shareholders and citizens are in for a rude awakening if organizations don't change and regain the control over trust they once had.

The journey to regaining control over trust will require bringing together process, policy, people and technology. Best practices, such as those from NIST on preparing and responding to CA compromises and on managing the key management lifecycle, are valuable. Guidance from regulators, such as the U.K. Information Commissioner's Office (ICO) on cloud computing and data privacy, also provide valuable frameworks for maintaining control over trust in the current and emerging age of computing. The ICO summarized a philosophy that CIOs and CEOs will do well to remember: "As a business, you are responsible for keeping your data safe. You can outsource some of the processing of that data, as happens with cloud computing, but how that data is used and protected remains your responsibility."[3] Finally, Forrester Research's *Kill Your Data to Protect It from Cybercriminals* is an excellent primer on defending data and trust in a world of evolving threats and highly motivated attackers.

Ultimately, as this research demonstrates, organizations' control over trust remains only as strong as their ability to manage cryptographic keys and digital certificates.

Endnotes

1 Boston Global, *Cost of data breach at TJX soars to $256m*, August 2007, http://bo.st/V608wu

2 Forrester Research, *Own Nothing. Control Everything*, January 2010

3   U.K. ICO, *Cloud on the horizon for data-handling outsourcing*, September 2012, http://bit.ly/ZnIfgC

Suggested resources:

The National Institute of Standards and Technology (NIST), *Preparing for and Responding to Certification Authority Compromise and Fraudulent Certificate Issuance*: http://csrc.nist.gov/publications/nistbul/july–2012_itl–bulletin.pdf

The National Institute of Standards and Technology (NIST), *Key Management Recommendations:* http://csrc.nist.gov/groups/ST/toolkit/key_management.html

UK Information Commissioners Office (ICO), *Guidance on the use of cloud computing* http://www.ico.gov.uk/news/latest_news/2012/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

Forrester Research, *Kill Your Data with Encryption, John Kindervag:* http://www.forrester.com/

Venafi guide to Enterprise Key and Certificate Management best practices: http://www.venafi.com/best–practices/

Ponem**o**n
INSTITUTE

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 www.ponemon.org.

About Venafi

Venafi is the inventor of and market leader in enterprise key and certificate management (EKCM) solutions. Venafi delivered the first enterprise-class solution to discover all keys and certificates, connect these assets to the people responsible for them, report on and audit their use to prove compliance, enforce policy to reduce risk and errors, and automate all operations to eliminate security risks, downtime and compliance failures. Venafi also publishes best practices for effective key and certificate management at www.venafi.com/best-practices. Venafi customers include the world's most prestigious Global 2000 organizations in financial services, insurance, high tech, telecommunications, aerospace, healthcare and retail. Venafi is backed by top-tier venture capital funds, including Foundation Capital, Pelion Venture Partners and Origin Partners. For more information, visit www.venafi.com.

Contact Venafi

If your enterprise is experiencing challenges related to trust technology management, specifically with regard to cryptographic keys and digital certificates, Venafi can assist. For more information about our products and services, visit us online at www.venafi.com. Or, contact us:

Utah Offices
126 W Sego Lily Drive #126
Sandy, UT 84070 USA
Phone +1.801.676.6900

New York Offices
1 Penn Plaza
53rd Floor
Suite 5328
New York, NY 10119

California Offices
Suite 202
530 Lytton Avenue
Palo Alto, CA 94301 USA
Phone +1 650.617.3223

UK Offices
Lily Hill House, Lily Hill Road
Bracknell, Berkshire RG12 2SJ
United Kingdom
Phone +44 (0) 1344 317980

Germany Offices
Einsteinstrasse 10
85716 Unterschleissheim
Germany
Phone +49 (89) 4161747–50

Finland Offices
Mannerheimintie 5
00 100 Helsinki
Finland

Brazil Offices
Market Place Torre II
Av. Dr Chucri Zaidan 940 – 16° andar
São Paulo, SP 04583–906, Brasil
Phone +55 11 5095 3519

Mexico Offices
Andrés Bello # 10 Colonia Chapultepec Morales
Del. Miguel Hidalgo
Mexico DF CP 11560, Mexico
Phone +52 55 3601 0764