NCSL - Cybersecurity Task Force

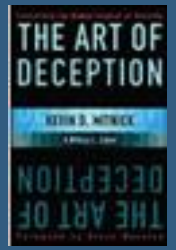
EMPLOYEE TRAINING & SECURITY AWARENESS

James Stanger
PhD, Chief Technology Evangelist
Computing Technology Industry Association (CompTIA)

Reggie Tompkins
Director, U.S. Public Sector Markets
Security Systems & Services Sales
IBM Corporation

Employee Training and Security Awareness

State of the Cybersecurity Industry – IBM and CompTIA & Research



Attack Methods – The Art of Deception

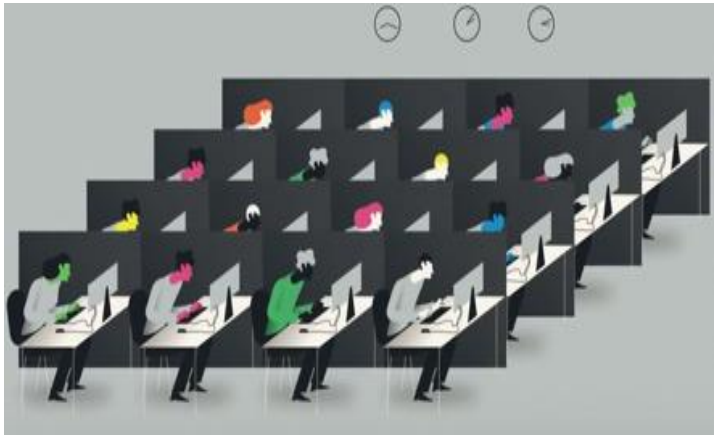
Role of The Employee

Employee Training and Security Awareness

State of the Cybersecurity Industry – IBM and CompTIA & Research

Cybercriminals and Their Motivations

Present: Organized & Professional



Why do *cybercriminals* and *adversaries* attack organizations?

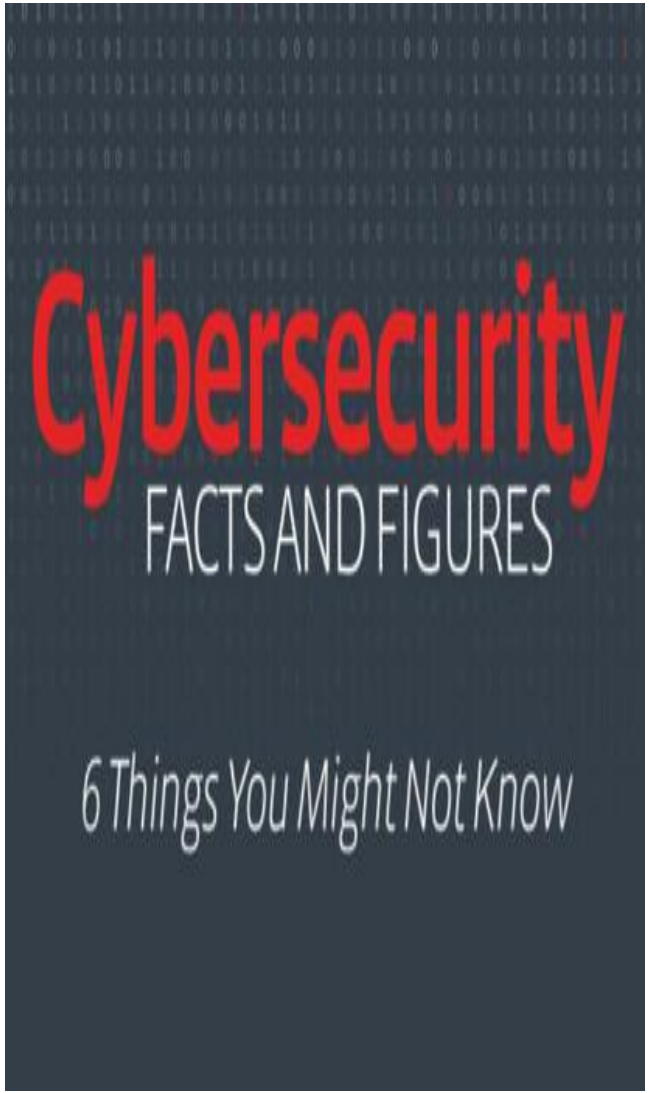
✓ **Financial gain:** According to the U.S. Treasury Department, worldwide cybercrime surpassed drug trafficking as the largest source of criminal revenue.

✓ **Industrial espionage:** Organizations spy on each other to steal industrial secrets for competitive advantage.

✓ **Political espionage:** Nations and nation-states continue to spy on each other, and they always will. Breaking into computers is just the latest technique available.

✓ **Military:** Like political espionage, competing military organizations want to know more about their military adversaries, and they have added cyberattacks as another means to gain needed intelligence or to sabotage military or industrial facilities.

✓ **Activism and hacktivism:** A lot of cyberattacks are aimed at disabling the online capabilities of organizations that the attackers disagree with on some social or ideological level.



- **By 2021, cybercrimes will cost $6 trillion per year worldwide.**
- **Businesses experience ransomware attacks every 40 seconds**
- **1 in 131 emails is malicious**
- **Attackers reside within a network for an average of 146 days before being detected**
- **Unfilled cybersecurity jobs will reach 3.5 million by 2021**
- **An IoT device can be attacked within 2 minutes**

Reference: ***CompTIA survey, "Value of Cybersecurity Professionals"***

https://certification.comptia.org/it-career-news/post/view/2017/10/04/6-stats-that-prove-the-value-of-cybersecurity-pros

Ransomware is most often delivered through e-mail, instant messaging, and even physical means.

Source: https://www.comptia.org/resources/cyber-secure-a-look-at-employee-cybersecurity-habits-in-the-workplace

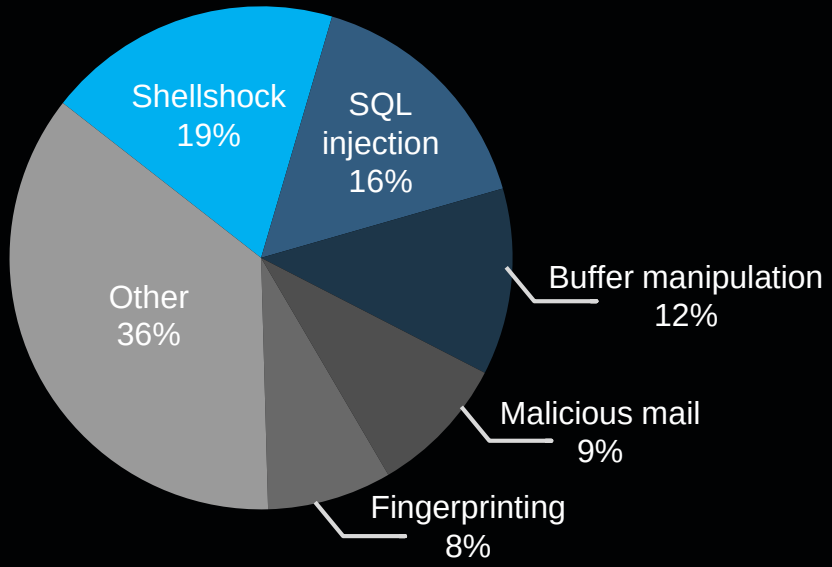
Any time employees interface with technology, they are susceptible to attack. So are your systems!

Most government attacks originate outside the organization, but inside attacks can be far more severe

71%
of attacks
committed by outsiders

29%
of attacks
committed by insiders

TOP ATTACK VECTORS



The vast majority of attacks begin with end users who get tricked into activating software

"The changing face of IT security in the government sector,"
IBM X-Force Research, December 2016.

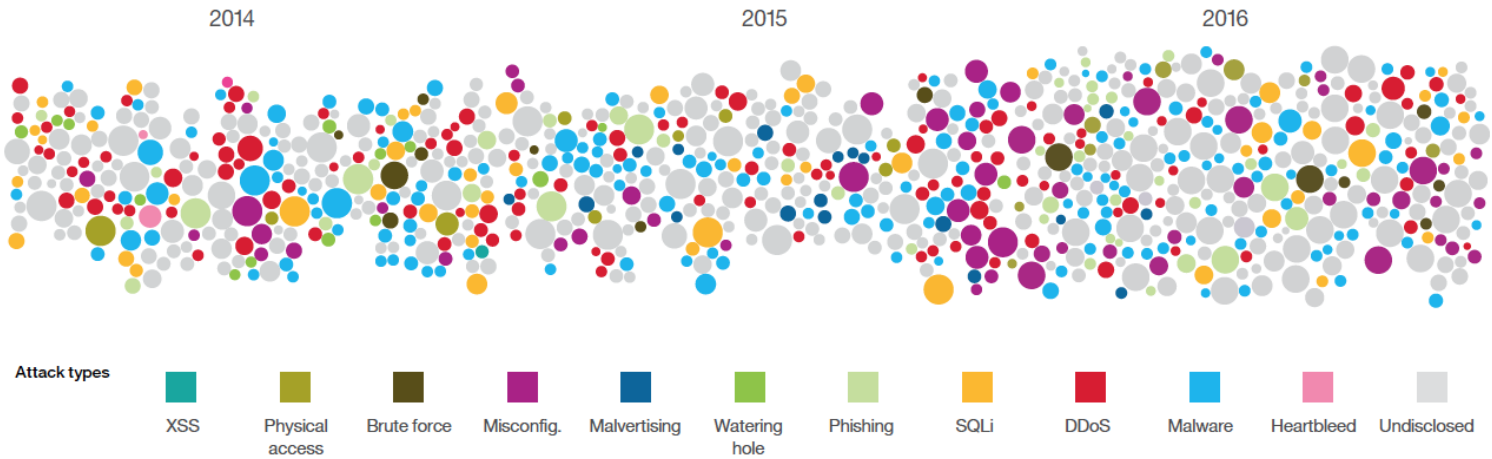
Security drivers are evolving

ADVANCED ATTACKS	INSIDERS	NEW INNOVATIONS	COMPLIANCE
From…			
• Broad threats • Individual hackers	• Disgruntled employees	• Technology and linear driven security strategy	• Checking the box • PCI compliance
To…			
• Targeted and organized crime (i.e., ransomware)	• Outsiders and partners becoming insiders	• Agile security that moves with the business	• Continuous risk analysis • GDPR
Cybercrime will become a **$2.1 trillion** problem by 2019	2016 insider attacks were **58 percent** 42% outsider attacks	By 2020, there will be **20.8 billion** connected "things"	GDPR fines can cost **billions** for large global companies
2015 Juniper Research Press Release	2017 IBM X-Force Threat Intelligence Report	2015 Gartner press release	2017 SecurityIntelligence.com article

Attackers break through conventional safeguards every day

Sampling of security incidents by attack type, time and impact, 2014 through 2016

Size of circle estimates relative impact of incident in terms of cost to business, based on publicly disclosed information regarding leaked records and financial losses.



IBM X-Force Threat Intelligence Report 2017

average time to detect APTs

191 days

average global cost of a data breach

$3.62M

2017 Cost of a Data Breach Study

Advanced Persistent Threat (APT): Unauthorized access over a long period of time that leads to stolen or altered data.

2017 Cost of a Data Breach Study global findings at a glance

$3.62M / 10%
Average total cost of data breach

$141 / 11.4%
Average cost per record lost or stolen

24,089 / 1.8%
Average number of breached records

27.7%
Likelihood of a recurring material breach over two years

419 companies participated
Currency: US dollar

Per-record costs for top three industries

$380 Health

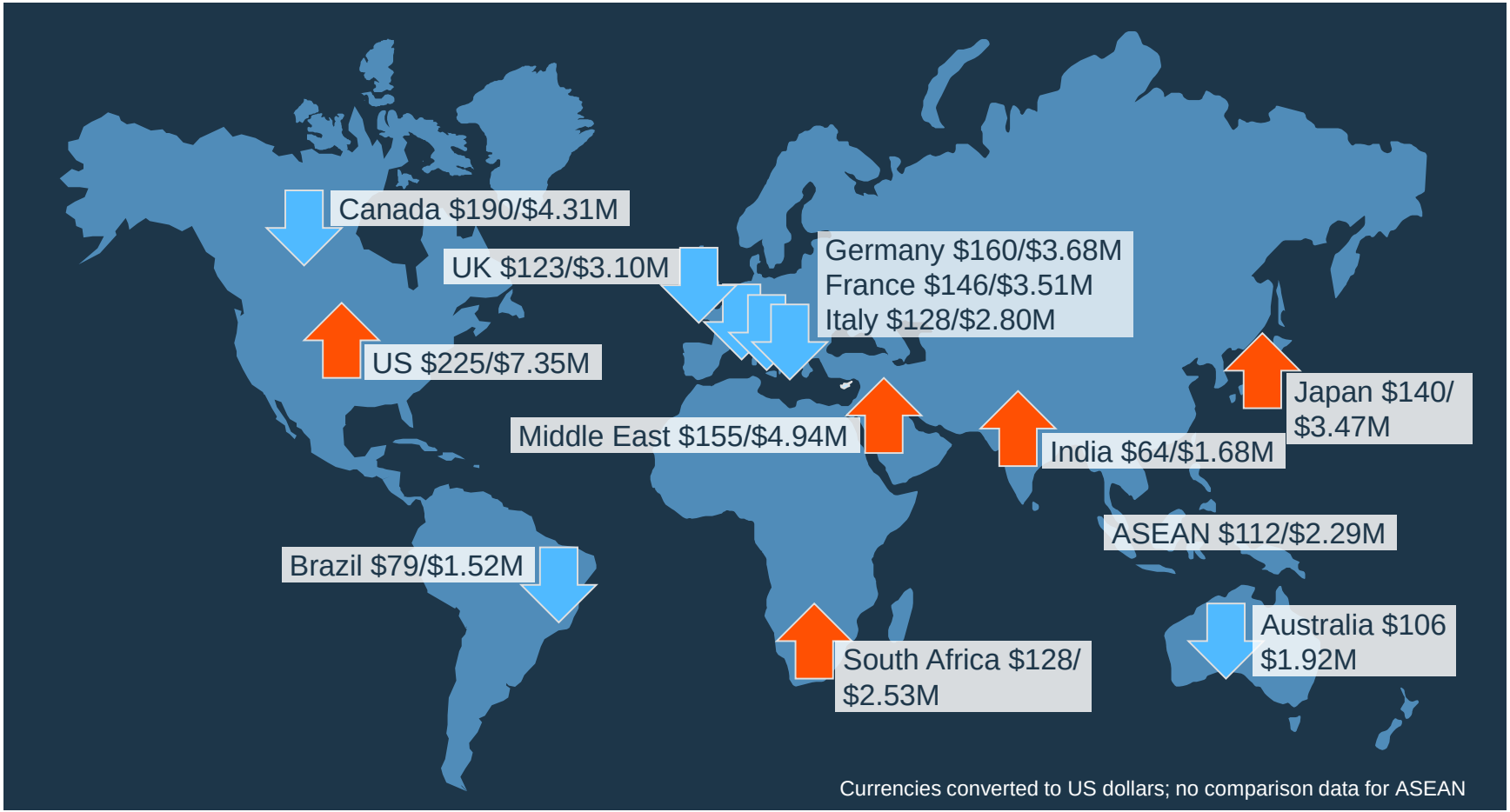
$245 Financial

$223 Services

2017 Cost of a Data Breach Study

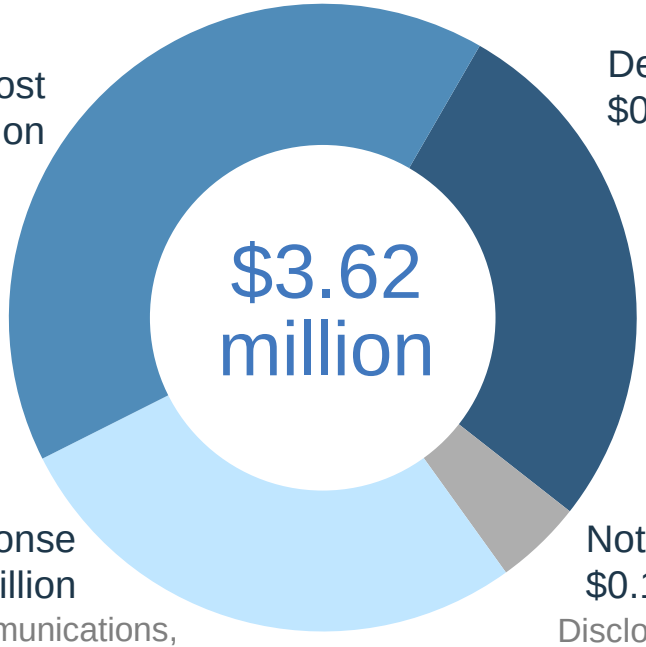
Costs and trends vary widely across countries

2017 Cost of a Data Breach Study



The largest component of the total cost of a data breach is lost business

Components of the $3.62 million cost per data breach



Lost business cost
$1.51 million
Abnormal turnover of customers, increased customer acquisition cost, reputation losses, diminished goodwill

Detection and escalation
$0.99 million
Forensics, root cause determination, organizing incident response team, identifying victims

Ex-post response
$0.93 million
Help desk, inbound communications, special investigations, remediation, legal expenditures, product discounts, identity protection service, regulatory interventions

Notification
$0.19 million
Disclosure of data breach to victims and regulators

2017 Cost of a Data Breach Study

Currencies converted to US dollars

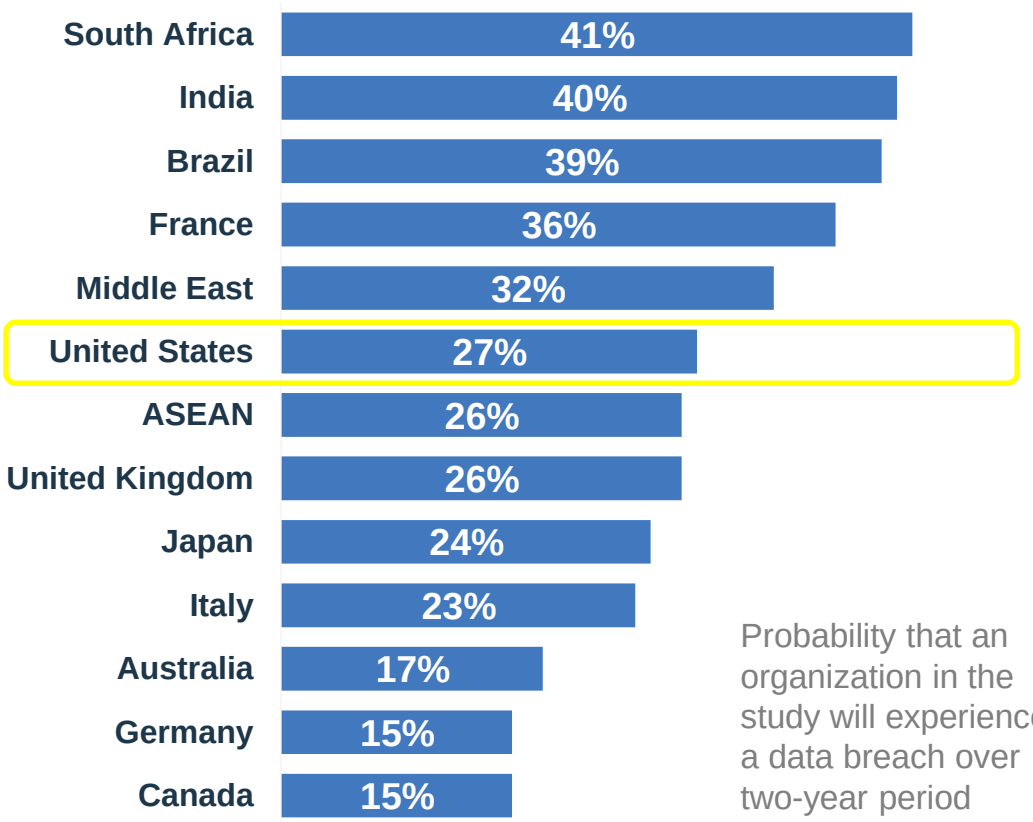
Odds of experiencing a data breach

2017 Cost of a Data Breach Study

Experiencing a data breach?

1 in 4

(Global average 28%)



Probability that an organization in the study will experience a data breach over two-year period

Security skills are more difficult to obtain and retain than ever

In-demand

73.9% of security professionals (compared to 60.7% of all IT pros) said they had been approached by a hiring organization or headhunter about job opportunities.

Overworked

Security professionals are more likely than other IT professionals (**64.5%** compared to **58.7%**) to report being under pressure to increase productivity and take on new tasks

Expensive

Information security manager is the hottest job boasting the biggest increase in average total compensation (up **6.4%** from 2015 to 2016).

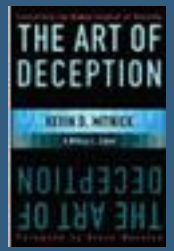
Source: 2016 Computerworld IT Salary Survey

Hard to replace

21% of jobs requiring **10+** years of experience take a year or more to fill and nearly half of jobs requiring **20+** years of experience take more than a year to fill.

Source: 2015 IDC Survey

Employee Training and Security Awareness



Attack Methods – The Art of Deception

Attack Methods

Social Engineering

Rogue Wi-Fi Access Point

Waterhole attack

Masquerading

Reconnaissance

Phishing

Distributed Denial of Service (DDOS) attack

Denial of Service (DDOS) attack

Baiting

Tailgating

Shoulder surfing

Rogue cell phone towers (interceptors, Stingray)

Spear phishing

Ransomware

Whaling

Pretexting

War driving / walking

Book: The Art of Deception

Don’t let a con artist steal from your firm by hoodwinking your people. ***The weakest link in your security system is probably the untrained employee*** — but you can fix that.

Takeaways

- Social engineers are skilled at influencing and persuading other people and they use those abilities to deceive your ***employees*** so they can steal your information.
- The weakest link in security systems is the human factor.
- Your ***employees*** are vulnerable to social engineers because they trust them and give out what they think is innocuous information.
- Most social engineers succeed because they have excellent people skills, and so they are very charming and likeable.
- Most people are willing to trust because they think deception is unlikely.
- If a deceiver gives a plausible reason, people don't become suspicious, even if they should.
- You should train your ***employees*** not to release any personal or internal company information unless they know the person and the person needs the information.
- Sometimes, to get information, an attacker will pose as someone who needs help.
- Control exactly what sensitive information you release.
- You can use verification and authorization systems to identify who gets information.

Employee Training and Security Awareness

Role of The Employee

3 Elements to a Comprehensive Employee Training & Security Awareness

- **Know Your Audience**

- **Pervasive Communications**

- **Interactive Education**

Key Challenges

- Information retention is a challenge with training programs that occurs infrequently.
- Interactive simulations produce higher levels of skills retention vs a presentation.
- Audiences are bored by education programs that fail to leverage a variety of media and content styles.
- As many as 91% of organizations provide cybersecurity training to their employees, yet 75% of those do so only at the time of hire or only as part of an annual “update. [1]

[1] “Building a Culture of Cybersecurity,” CompTIA, April 2018

Recommendations

- Assess the culture of the enterprise to determine requirements for the specific messaging, delivery and frequency of security awareness and training.
- Implement an attack simulation program such as a phishing simulation program, deliver social engineering attacks with corresponding just-in-time training and teachable moments.
- Use communications and marketing tools for ongoing reinforcement – keep security top-of-mind.

Blue Demonstration

Thank you!

Questions?

James Stanger, PhD
Chef Technology Evangelist,
CompTIA
jstanger@comptia.org
+1 (360) 970-5357
Twitter: @jamesstanger
Skype: stangernet
James CompTIA Hub:
https://certification.comptia.org/it-career-news/hub/James-Stanger

Reginald Tompkins
Director, U.S. Public Sector Markets
IBM
rdtompk@us.ibm.com
+1 (770) 713-8184
www.ibm.com

Government is now a prime target for ransomware attacks

Ransomware attacks increased by more than

300%

in the government sector from 2015 to 2016[1]

19%

of ransomware attacks targeted government in 2016[2]

52%

Companies and government entities who recognize that human error is increasing[3]

INCIDENT RESPONSE

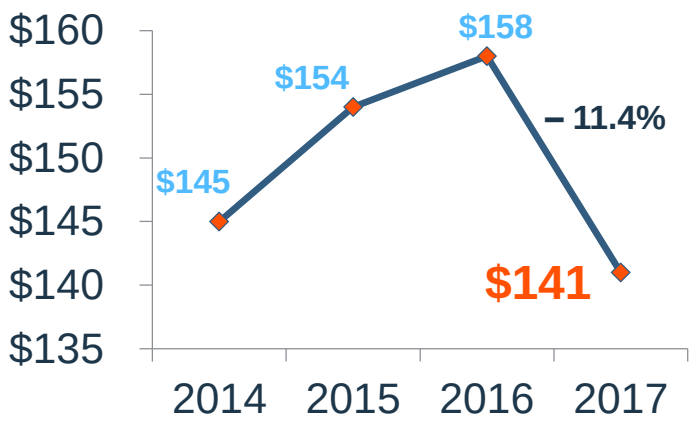
- Development of a response plan and policy for ransomware attacks
- Long-overdue operating system updates and patches
- Isolation of infected devices
- Mandated adherence to corporate security standards for personal devices
- Vulnerability scanning to identify exposures and defend against future attacks

[1] "The Rising Face of Cyber Crime: Ransomware," BitSight Technologies, 2016.
[2] "Global Threat Intelligence Report 2017," NTT Security, 2017.
[3] "CyberSecure Human Error White Paper," CompTIA 2017.

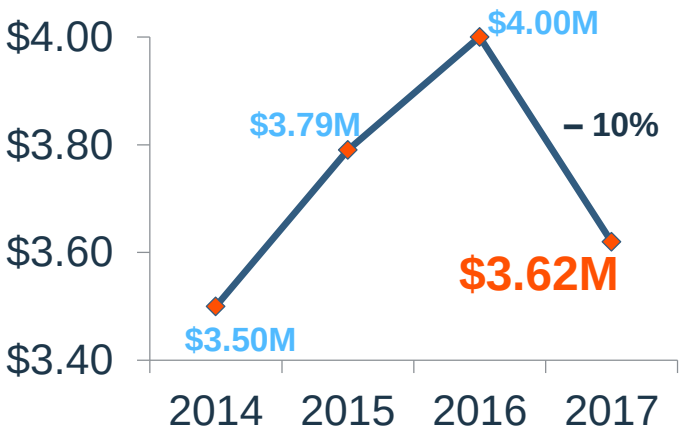
What goes up should come down

- The global average cost of a data breach is down over previous years
- 48% of the per-record 11.4% decrease over last year is due to the US dollar exchange rate
- The average size of a data breach increased 1.8% to 24,089 records

Global average cost per record
in US dollars



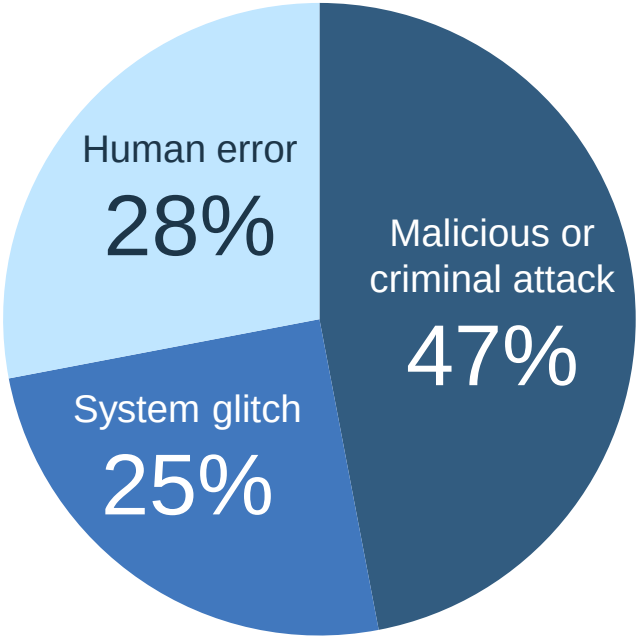
Global average cost per incident
in millions of US dollars



2017 Cost of a Data Breach Study

Humans, hackers and criminal insiders continue to cause most data breaches

$126
per record to resolve



$156
per record to resolve

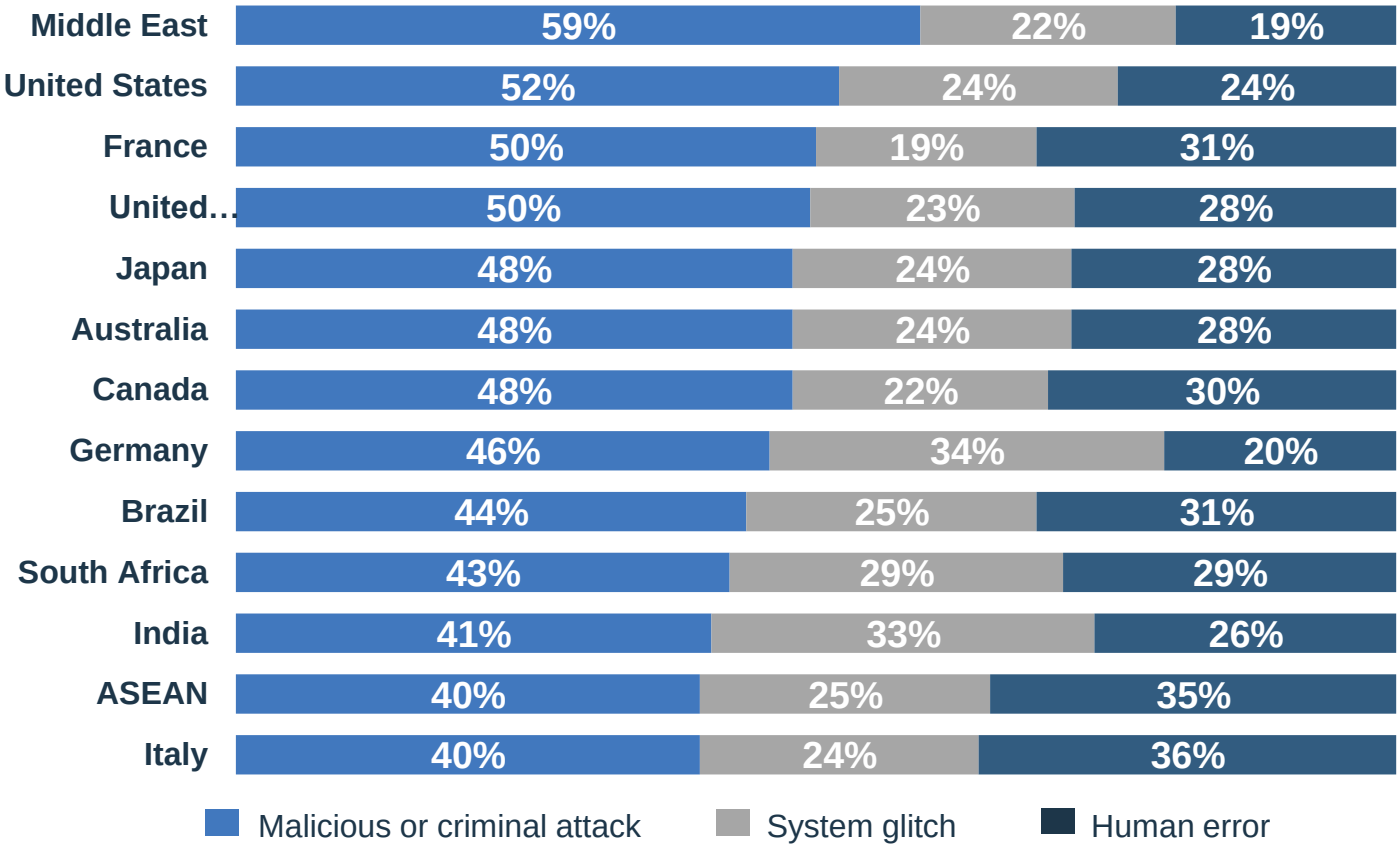
$128
per record to resolve

Currencies converted to US dollars

2017 Cost of a Data Breach Study

The incidence of malicious attack varies considerably by country

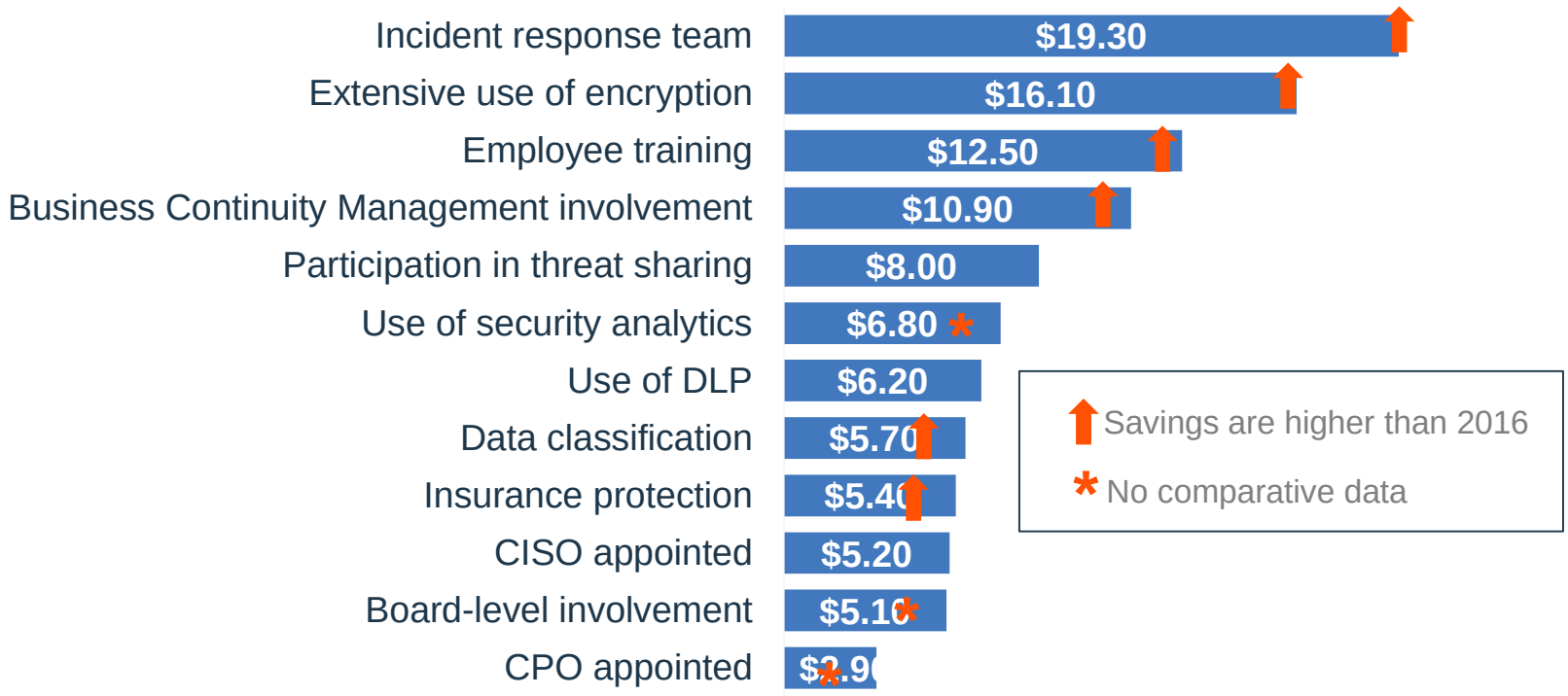
2017 Cost of a Data Breach Study



What you can do to help reduce the cost of a data breach

Amount by which the cost-per-record was lowered

2017 Cost of a Data Breach Study



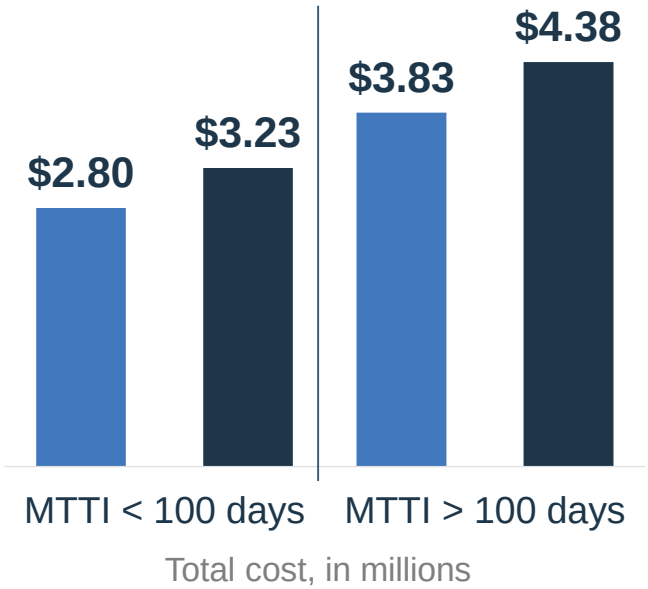
Currencies converted to US dollars

Gaining visibility and responding faster help to reduce costs

2017 Cost of a Data Breach Study

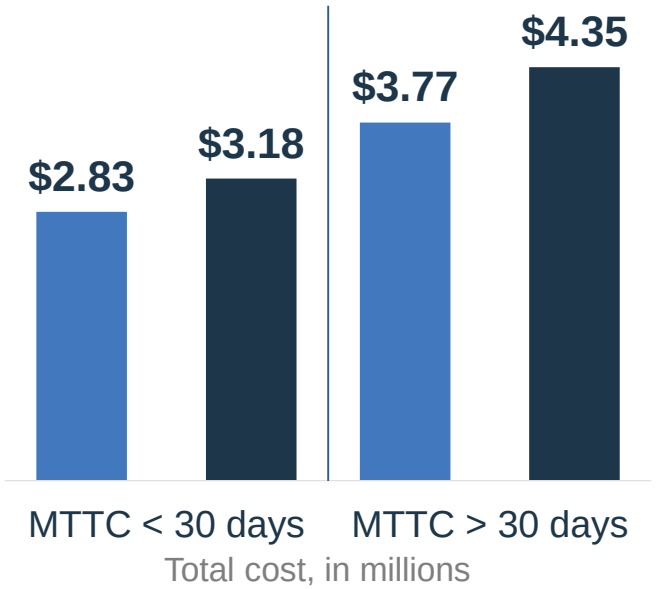
Mean time to identify (MTTI)

(The time it takes to detect that an incident has occurred)



Mean time to contain (MTTC)

(The time it takes to resolve a situation and ultimately restore service)



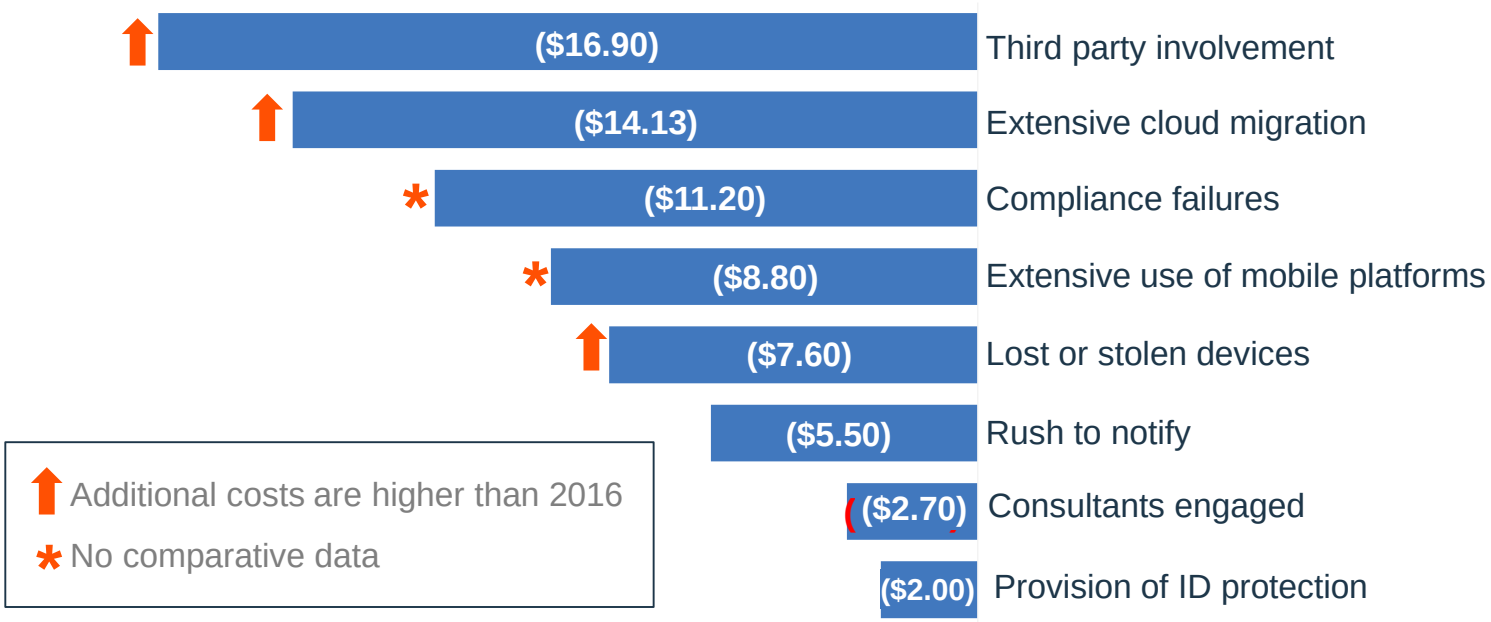
FY 2017 FY 2016

Currencies converted to US dollars

Factors that increase the per-record cost

2017 Cost of a Data Breach Study

Amount by which the cost-per-record was increased



Currencies converted to US dollars