# Cybersecurity Landscape and Risk Considerations

## Managing Risk in a Digital Business Environment

nuix
Simple. Powerful. Precise.

Russ Berkoff
SVP, Cybersecurity, Intelligence, and Investigative Services
May 2018 - AFCEA

Today the U.S. finds itself in a paradoxical position… "uniquely powerful and vulnerable" when it comes to the competition in cyberspace

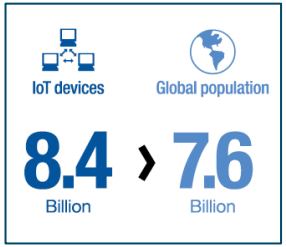
It wields a dominant position in the fields of hardware, software, and offensive cyber capabilities. But the U.S. is so connected to the Internet that its cyber borders are too many, too diverse and too poorly guarded to secure effectively

-- Adam Segal, *The Hacked World Order*, 2016

nuix

# Pervasive and complex in nature… Cybercrimes are projected to destroy $6 trillion of economic value by 2021[1]

- Former NSA Director, General Keith Alexander calls cyber theft of intellectual property ***"the greatest transfer of wealth in human history."***
- **Cybercrime** continues to fuel cybersecurity market growth
- Cybersecurity **spending to exceed $1 trillion from 2017-2021**
- **Human attack surface to reach 6 billion people by 2022**… there were 3.8 billion internet users in 2017 (51% of the world's pop. of 7 billion)
- Global **ransomware** damage costs are predicted to **exceed $5 billion in 2017**
  - Ransomware attacks on **healthcare** organizations is No. 1 attacked industry
  - Ransomware damage **costs will rise to $11.5 billion in 2019**
- Cybercrime will more than **triple the number of unfilled cybersecurity jobs,** which is predicted to reach 3.5 million by 2021




[1]Cybersecurity Ventures

nuix

# Cyberattacks targeting critical infrastructure and strategic industrial sectors are on the close horizon

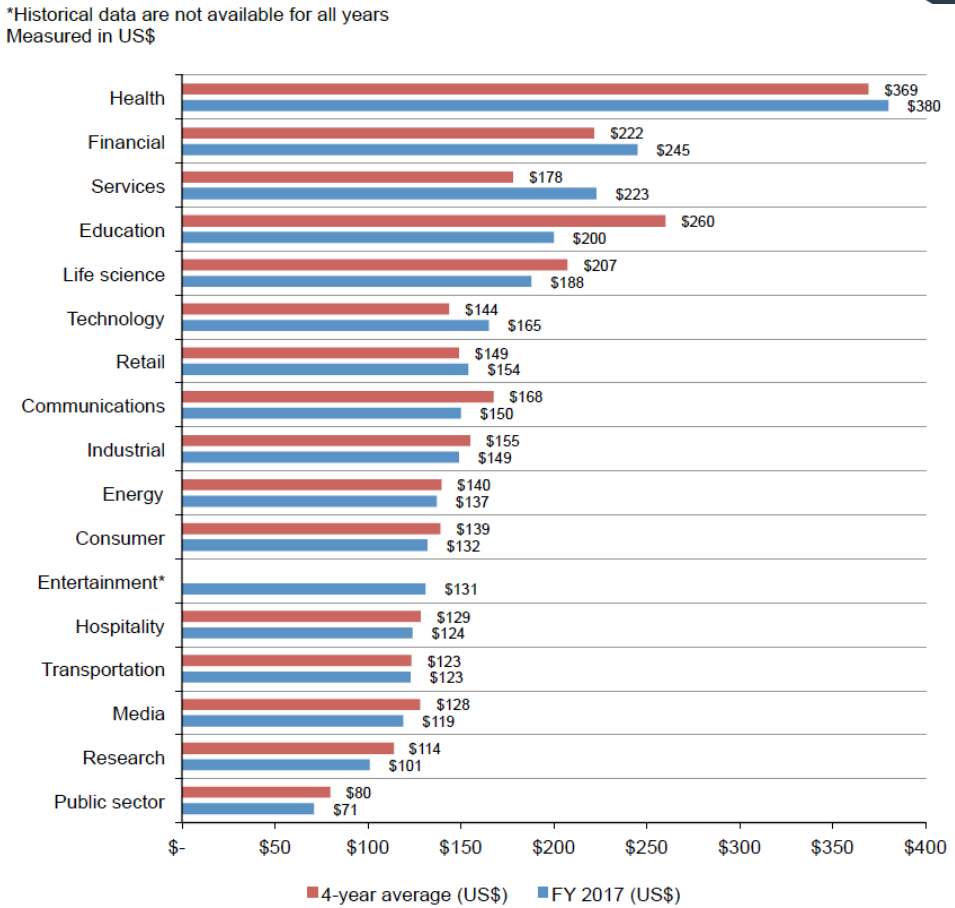
- Cybersecurity **risks growing** both in prevalence and in disruptive potential
- **Attacks** against businesses - **doubled in five years**
    - Incidents once considered extraordinary becoming commonplace
- **Financial impact** of cybersecurity breaches is **rising**
    - Some of **largest costs** in 2017 related to **ransomware** attacks, accounting for 64% of all **malicious emails**
    - WannaCry attack… affecting 300,000 computers across 150 countries—and NotPetya … caused quarterly losses of US $300 million

Sources: World Economic Forum, 2018

# Industry Costs – Data Breach

## Per capita cost by Industry

- **Heavily regulated industries** cost substantially higher than overall mean $141
- **Public sector**, research, media and transportation cost well under overall mean




Sources: Ponemon/IBM Study, 2017

# Malicious Attacks are Costlier

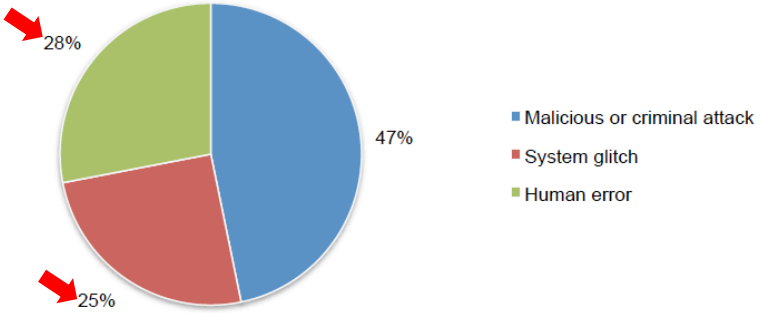
Most common types of malicious or criminal attacks

- Malware infections
- Criminal insiders
- Phishing/social engineering and SQL injection

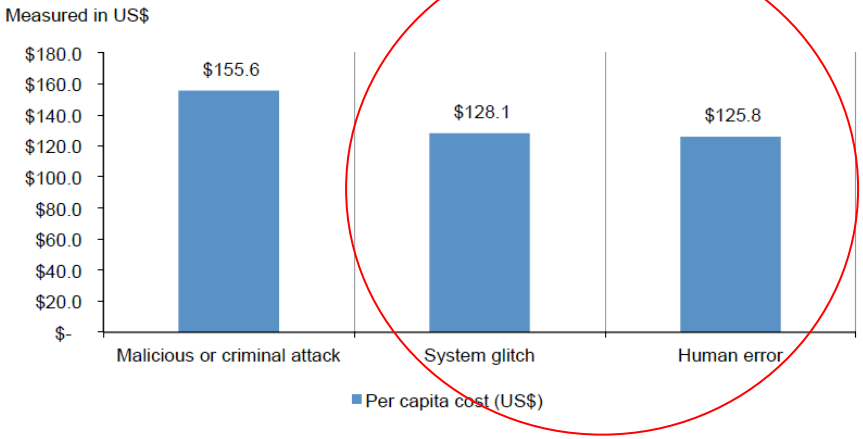
**Non-malicious activity still 53% root cause**

- **System Glitches & Human Error**

Distribution of the benchmark sample by root cause of the data breach




Per Capita Cost for three root causes of the data breach



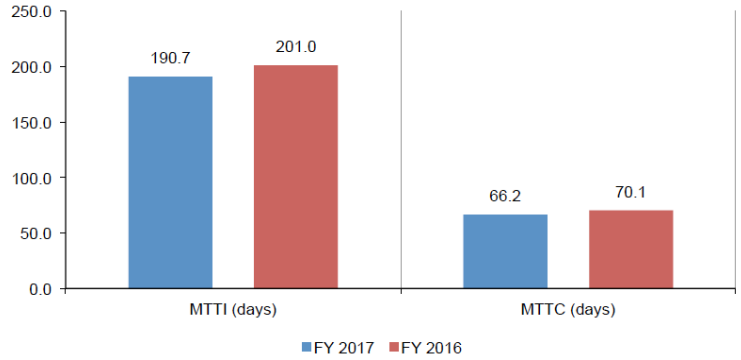

Sources: Ponemon/IBM Study, 2017

# Time to identify breach is getting faster

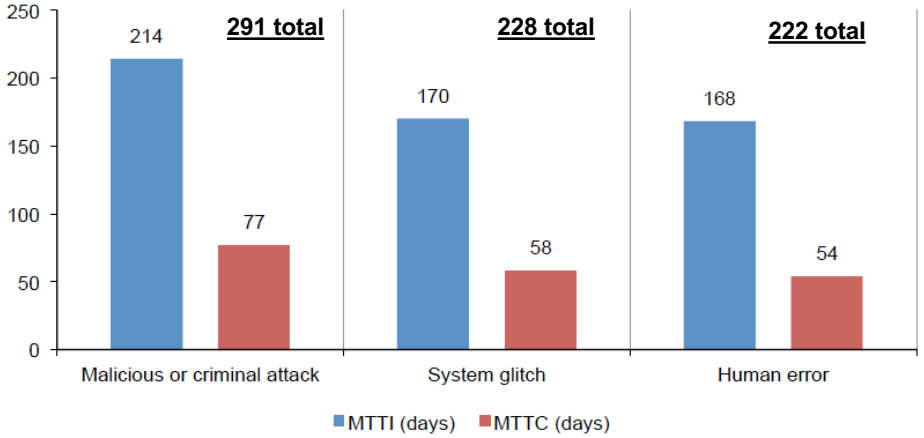
- 191 days to identify a breach
- 66 days to contain the breach

**257 days vs. 271 days** (14 days faster)

Days to identify and contain data breach over the past year



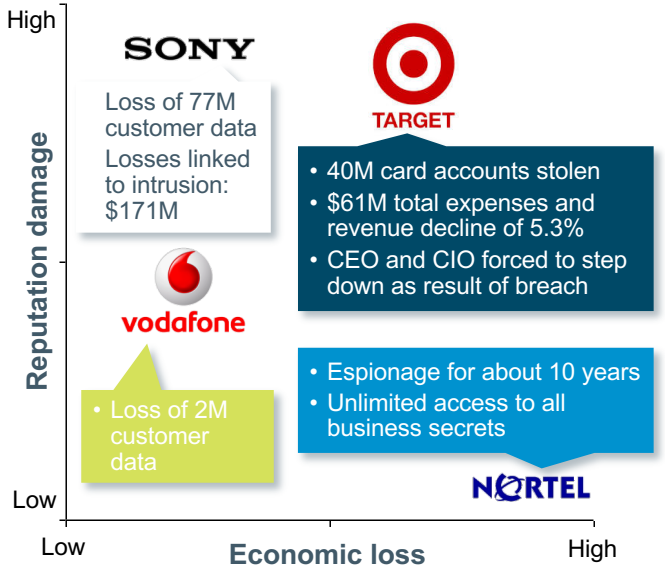

Days to identify and contain data breach incidents by root cause




Sources: Ponemon/IBM Study, 2017. MTTI: Mean Time to Identification, MTTC. Mean Time to Change

# The commercial impact from exposed breaches affects both a company's bottom line and reputation

**Example impacts of Cybersecurity breaches**




- **Loss of customers increased cost of data breach**
- Analysis shows that **95% of all companies** are currently **under at least partially successful attack**
- The **most dangerous attacks are those which remain undetected** for a long time
  - Average time to discovering breaches are > 191 days

Sources: Ponemon/IBM Study, 2017

## Numerous industries have adapted to corporate risk and costs of cyber attacks making cybersecurity an entire enterprise issue

- Impact of cyber-attacks may extend far beyond direct costs associated with immediate response to an attack
- Corporate **responsibilities and accountability shifting to C-suite/Board** for more direct management and risk oversight to meet fiduciary and legal obligations

### Sources of Cybersecurity Risk

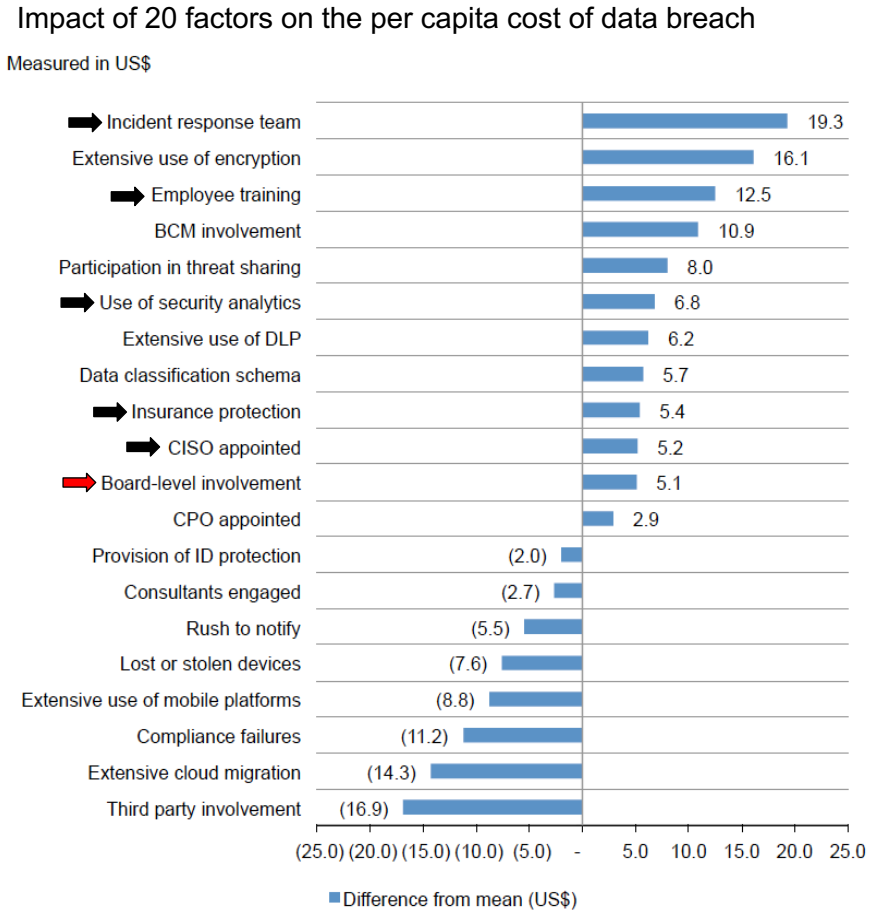
- Breaches of personal data both customer and employee
- Breaches of business proprietary data
- Introduction into internal networks viruses or other malicious code
- Introduction of other vulnerabilities to IT systems
- Misuse and secondary use of company data
- 4th party risk – relationship with their 3rd party vendors
- Potential director or management liability for breech of fiduciary duty in cybersecurity oversight

### Significant Corporate Costs

- Reputational damage
- Intellectual property
- Sensitive business information (i.e. M&A)
- Privacy liability
- Identity theft
- Physical property
- Business operations
- Additional costs to secure exposed networks

Source: SEC 2014 & Marsh 2014, Navigating the Digital Age/2015

## Global megatrends in cost of data breach findings




Sources: Ponemon/IBM Study, 2017

nuix

# Cybersecurity implications are ubiquitous, forcing organizations to make sophisticated risk trade-offs… and making it a business imperative

- ***"Cybersecurity touches every business process and function, not only in operations but also in customer care, marketing, product development, procurement, human resources, and public affairs"***[1]
- Numerous institutions have begun to make **cybersecurity a key part of business strategy** beyond technology governance[1]
- **Senior leaders are having to define the risk appetite of their organization** for loss of intellectual property, disclosure of customer information, and business disruption[2]
- **A business-driven cybersecurity model has emerged** to provide resilience across both technical and risk functions… considering employee, customer, and 3rd party accesses[1]
- **Senior management's time and attention** was identified as the single biggest driver of maturity in managing cybersecurity risks[3]
- It is important we discern the complex requirements emerging from **increased regulatory constraints** on private sector activities within these new security dynamics

1. SEC, Guidance Update, 4/15
2. SEC Commissioner Luis A. Aguilar, Cyber Risk and the Boardroom, 6/14
3. McKinsey, Why senior leaders are the front line against cyberattacks, 6/14

# Boards risk litigation and regulatory scrutiny from breaches, resulting in substantial legal fees & major distractions

## Legal implications of recent cyber breaches:

- 4 lawsuits filed against 13 directors, and officers
- Settlement >$67M

TARGET

- 12 lawsuits against directors and officers
- Breach led to as many as 44 consumer civil actions

THE HOME DEPOT

- Lawsuit named 10 directors and officers as defendants asserting claims for breach of fiduciary duty, waste of corporate assets, and unjust enrichment.
- Losses linked to intrusion $171M

WYNDHAM HOTEL GROUP

Consumer, bank and shareholder suits
Cost $32M

Heartland

## Landmark Delaware Cases are beacons for directors:

- Directors & Officers **must not demonstrate a "conscious disregard"** for their duties or ignore red flags
- Conduct that evidences **lack of good faith may violate fiduciary duty of loyalty**

## Growing Regulatory Scrutiny:

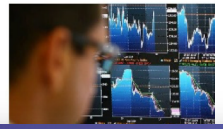
- **EU –** New **PII data protection rules and penalties,** and **"Right to Forget"** standards, May 2016, GDPR – May 2018
- **FTC** – Enforces data security federal statutes and regulations - **58 settlements to date** with increasing trend
- **FCC** – 2014 – first two companies **fined $10M each** for maintaining "unjust and unreasonable" data security practices
- **SEC** – Issued guidance… **Be pro-active**... approach cybersecurity enterprise-wide... boards must define who is responsible for cybersecurity, **disclosure** of cybersecurity events
- **NIST** – **Mandatory cybersecurity framework** for organizations deemed part of nation's critical infrastructure
- **States Attorney Generals** are **enforcing both state and federal statutes** against companies within their jurisdictions

# Security and GDPR Concerns

June 15, 2017

## Report predicts banks to get €4.7bn fines in first 3 years under GDPR

*Report urges banks to focus on breach response readiness to mitigate GDPR risk as predicted number levels of fines are exceedingly highs.*



A new report is "conservatively" forecasting that European finance organisations are about to shell out €4.7 billion in first three years after the GDPR comes into power thanks to data breaches which they don't currently have to declare.

Consult Hyperion, which commissioned AllClear ID to carry out the research said in a press release, "this forecast is conservative compensation claims, costs associated with lost customers, d reputations and senior executive resignations."

SC Media UK asked Consult Hyperion how the report reache and a spokesperson for the firm said the stats were, "gathere

BUSINESS

## Google Faces Record EU Antitrust Fine

Penalty could reach as high as 10% of annual revenue, which was more than $90 billion in 2016

JUNE 16, 2017


## *E.U. Fines Facebook $122 Million Over Disclosures in WhatsApp Deal*

MAY 18, 2017

## TalkTalk hit with record fine over cyber attack

OCTOBER 15, 2016

# EU GDPR Requirements

## GDPR will have critical implications across every organization's enterprise

GDPR
EU General Data Protection Regulation


**PROFILING ACTIVITIES**
Big data analytics will require explicit consent from the subjects

**OUTSIDE OF THE EU?**
Activities directed at EU residents, even if by non EU entities, are covered

**DATA PROTECTION OFFICERS**
Data controllers and processors must designate a Data Protection Officer

**BREACH NOTIFICATIONS**
Personal data breaches must be notified to the regulatory body by the DPO within 72 hrs

**WHAT IS A BREACH?**
The regulation states a "personal data breach" is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

**PROCESSING OF PERSONAL DATA**
Consent mechanisms may be required for data collection and processing

**DEEPER 'PERSONAL' DATA POOL**
Will include IP addresses, genetic data, data from cookies and will affect profiling activities

**BIG FINES**
Penalties start at the greater of €10m or 2% of gross revenue rising to €20m and 4% of gross revenue

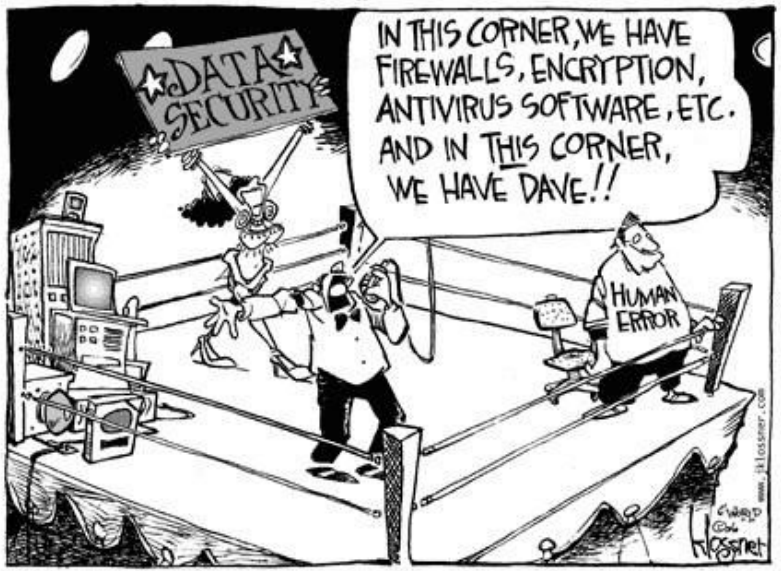
nuix

# Prediction… 3.5 million unfilled cybersecurity jobs are expected by 2021[1]

- Demand for cybersecurity professionals increases to **6 million globally by 2019**[2]
- The sheer volume of cyberattacks triaged daily **nearly impossible for humans to keep pace**[3]
- The cybersecurity workforce shortage has left CISOs and corporate IT security teams shorthanded… **scrambling for talent while cyber attacks intensify**
- Every IT worker, **every technology worker, needs to be involved** with protecting and defending apps, data, devices, infrastructure, and people
- **Technology is essential** without a sufficient army of white hats (good guys)

[1]Cybersecurity Ventures. [2] Palo Alto Networks Research Center [3] Microsoft's Global Incident Response and Recovery Team. World Economic Forum, 2018

# It’s about people, not just technology




Simple. Powerful. Precise.

Russ Berkoff

SVP, Cybersecurity, Intelligence and Investigation Services

russ.berkoff@nuix.com

Mobile:  (410) 262-4614