CHELSEA
TECHNOLOGIES

# ASA/AFRA 2017 CONFERENCE

## CYBERSECURITY NEWS

ASA RESTON, VA · AFRA 9-11 JULY 2017 · parts · distribution · disassembly · recycling

**JULY 2017**

**Meyer Ben-Reuven – meyer@chelsea-tech.com**

# CYBERSECURITY MYTHS

*MYTH 1:* I don't go to dangerous sites, and I check my links, so I'm safe.

*MYTH 2:* My anti-virus is up to date, so I'm safe.

*MYTH 3:* Infected computers display nasty messages and are very slow.

*MYTH 4:* Our systems are proprietary, hackers don't know the communication protocols.

*MYTH 5:* We have a firewall. We're in good shape.

*MYTH 6:* Our systems are disconnected from the Internet, so we don't have any risk.

*MYTH 7:* Hackers are not interested in water and wastewater systems.

*MYTH 8:* We trust our vendors and integrators to implement safe systems.

*MYTH 9:* Our cybersecurity is handled by our IT department. It's too complicated for management to get involved.

*MYTH 10:* We don't have the money to implement a cybersecurity program.

*MYTH 11:* We are a small company – who would want our data?

# CYBERSECURITY HISTORY

## The first recorded cyber crime took place in the year 1820.

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime!

# CYBERSECURITY WAR

## We are not prepared for Cyber War – but it is an Economic War

Focus on High Value Targets
Sophistication of Attack Techniques
Breaches without Borders
A Need for Security Basics

# CYBERSECURITY CHALLENGES

## CISOs face a shortage of skills, lack of metrics and strategy

Security Maturity
Board of Directors
Stakeholders
Compliance Mandates
Industry Standards

**49%** of IT executives have **no measure of security effectiveness**

2012 Forrester Research Study

**31%** of IT professionals have **no risk strategy**

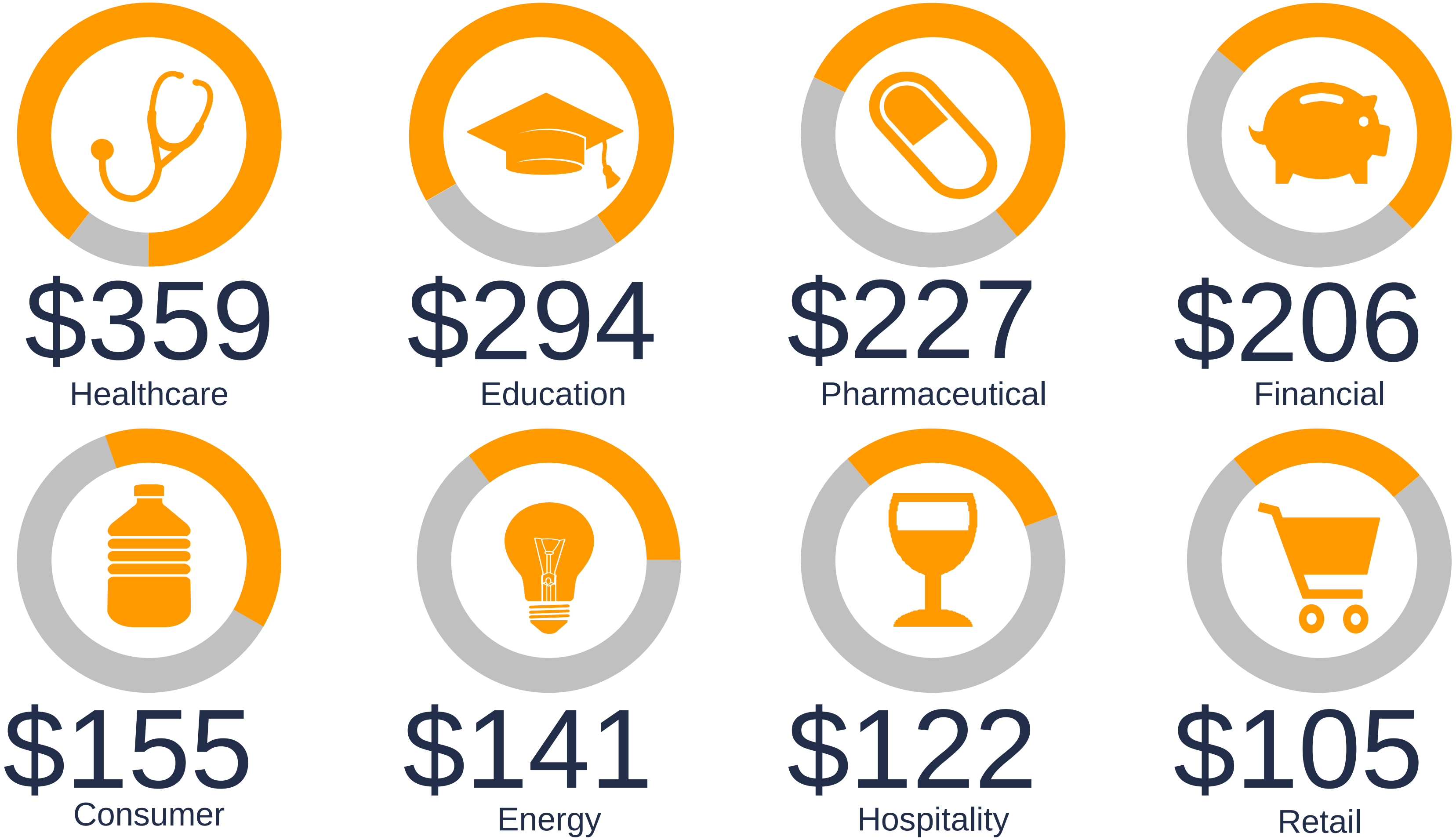
2013 Global Reputational Risk & IT Study, IBM

**83%** of enterprises have difficulty finding the **security skills** they need

*2012 ESG Research*

# CYBERSECURITY BREACH COSTS

## Highly regulated industries have highest per-record data breach costs



$359 Healthcare

$294 Education

$227 Pharmaceutical

$206 Financial

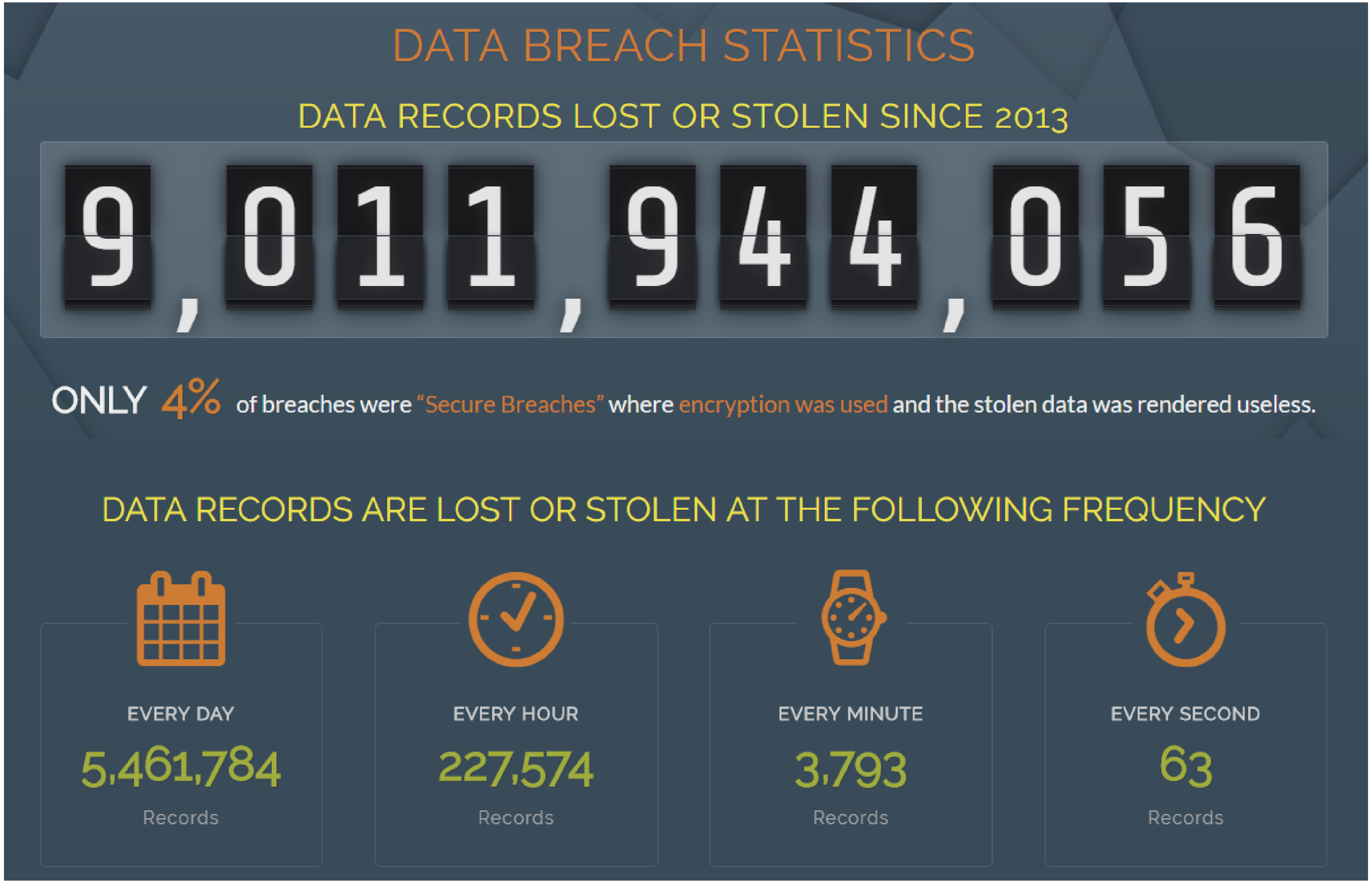
$155 Consumer

$141 Energy

$122 Hospitality

$105 Retail

# CYBERSECURITY BREACH STATS



## DATA BREACH STATISTICS

DATA RECORDS LOST OR STOLEN SINCE 2013

9,011,944,056

ONLY 4% of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.

DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY

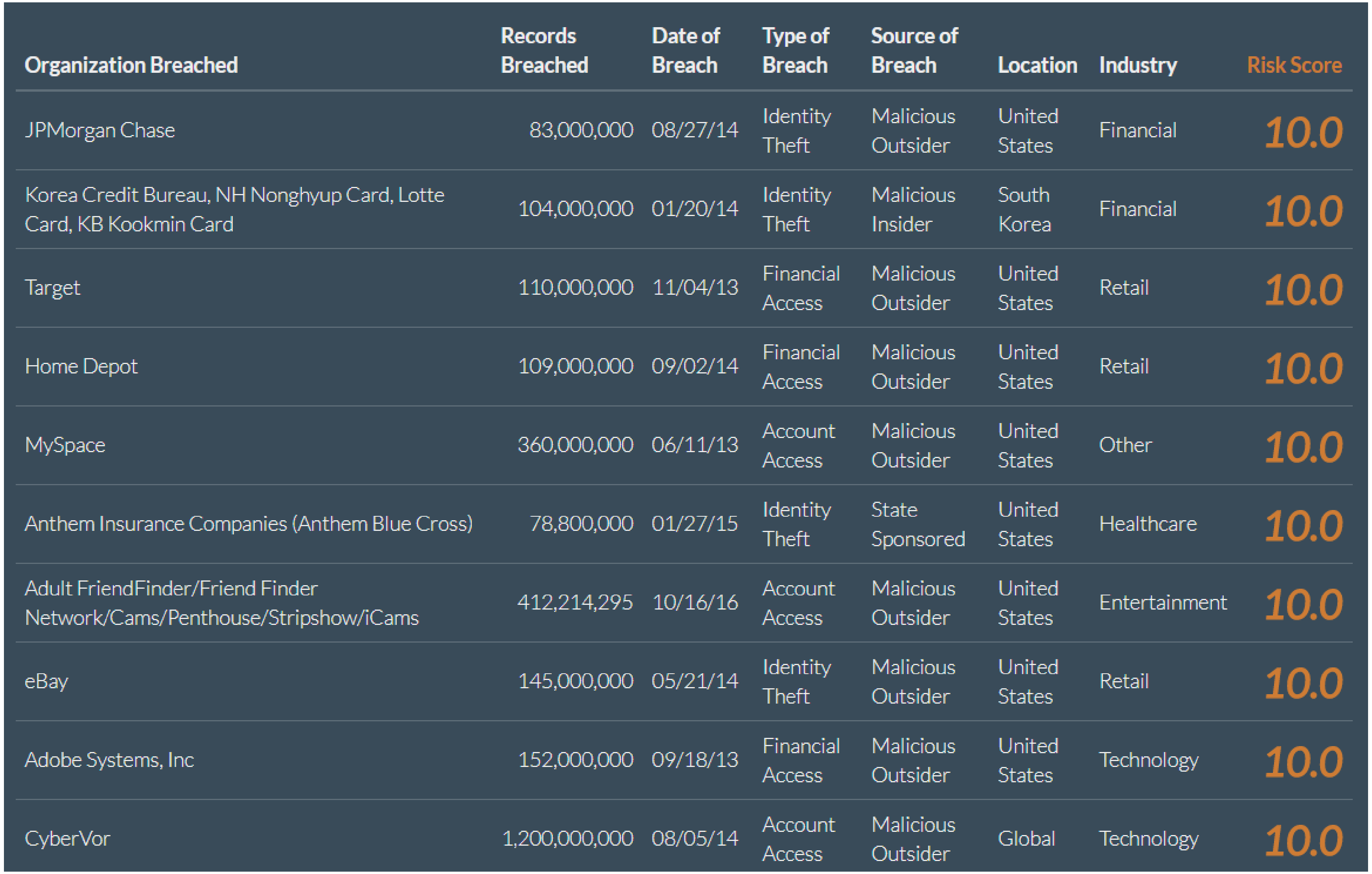
EVERY DAY
5,461,784
Records

EVERY HOUR
227,574
Records

EVERY MINUTE
3,793
Records

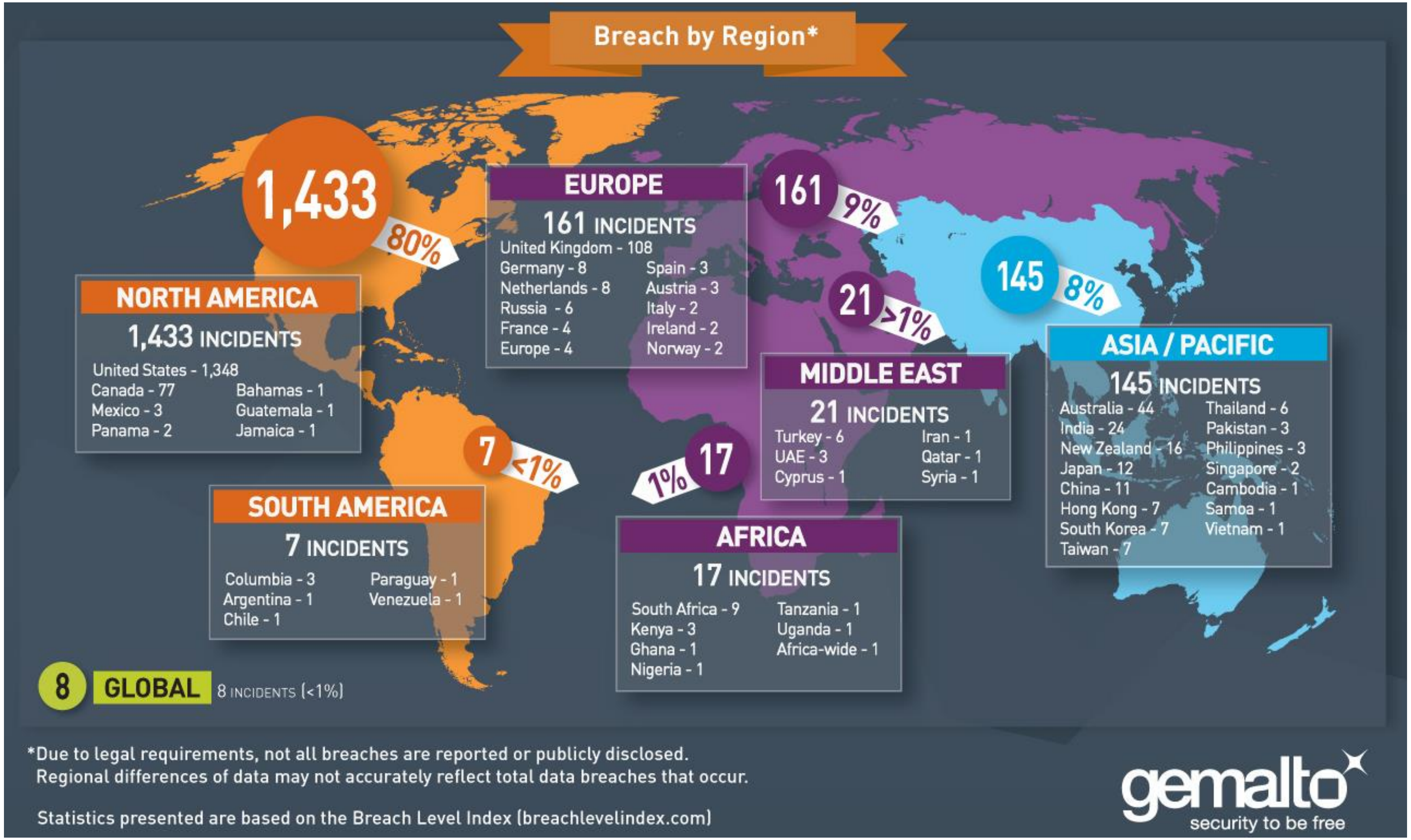
EVERY SECOND
63
Records

# TOP SCORING DATA BREACHES



| Organization Breached | Records Breached | Date of Breach | Type of Breach | Source of Breach | Location | Industry | Risk Score |
|---|---|---|---|---|---|---|---|
| JPMorgan Chase | 83,000,000 | 08/27/14 | Identity Theft | Malicious Outsider | United States | Financial | 10.0 |
| Korea Credit Bureau, NH Nonghyup Card, Lotte Card, KB Kookmin Card | 104,000,000 | 01/20/14 | Identity Theft | Malicious Insider | South Korea | Financial | 10.0 |
| Target | 110,000,000 | 11/04/13 | Financial Access | Malicious Outsider | United States | Retail | 10.0 |
| Home Depot | 109,000,000 | 09/02/14 | Financial Access | Malicious Outsider | United States | Retail | 10.0 |
| MySpace | 360,000,000 | 06/11/13 | Account Access | Malicious Outsider | United States | Other | 10.0 |
| Anthem Insurance Companies (Anthem Blue Cross) | 78,800,000 | 01/27/15 | Identity Theft | State Sponsored | United States | Healthcare | 10.0 |
| Adult FriendFinder/Friend Finder Network/Cams/Penthouse/Stripshow/iCams | 412,214,295 | 10/16/16 | Account Access | Malicious Outsider | United States | Entertainment | 10.0 |
| eBay | 145,000,000 | 05/21/14 | Identity Theft | Malicious Outsider | United States | Retail | 10.0 |
| Adobe Systems, Inc | 152,000,000 | 09/18/13 | Financial Access | Malicious Outsider | United States | Technology | 10.0 |
| CyberVor | 1,200,000,000 | 08/05/14 | Account Access | Malicious Outsider | Global | Technology | 10.0 |

# CYBERSECURITY BREACH BY REGION



## Breach by Region*

### NORTH AMERICA

1,433 INCIDENTS

| | |
|---|---|
| United States - 1,348 | |
| Canada - 77 | Bahamas - 1 |
| Mexico - 3 | Guatemala - 1 |
| Panama - 2 | Jamaica - 1 |

### EUROPE

161 INCIDENTS

| | |
|---|---|
| United Kingdom - 108 | |
| Germany - 8 | Spain - 3 |
| Netherlands - 8 | Austria - 3 |
| Russia - 6 | Italy - 2 |
| France - 4 | Ireland - 2 |
| Europe - 4 | Norway - 2 |

### MIDDLE EAST

21 INCIDENTS

| | |
|---|---|
| Turkey - 6 | Iran - 1 |
| UAE - 3 | Qatar - 1 |
| Cyprus - 1 | Syria - 1 |

### ASIA / PACIFIC

145 INCIDENTS

| | |
|---|---|
| Australia - 44 | Thailand - 6 |
| India - 24 | Pakistan - 3 |
| New Zealand - 16 | Philippines - 3 |
| Japan - 12 | Singapore - 2 |
| China - 11 | Cambodia - 1 |
| Hong Kong - 7 | Samoa - 1 |
| South Korea - 7 | Vietnam - 1 |
| Taiwan - 7 | |

### SOUTH AMERICA

7 INCIDENTS

| | |
|---|---|
| Columbia - 3 | Paraguay - 1 |
| Argentina - 1 | Venezuela - 1 |
| Chile - 1 | |

### AFRICA

17 INCIDENTS

| | |
|---|---|
| South Africa - 9 | Tanzania - 1 |
| Kenya - 3 | Uganda - 1 |
| Ghana - 1 | Africa-wide - 1 |
| Nigeria - 1 | |

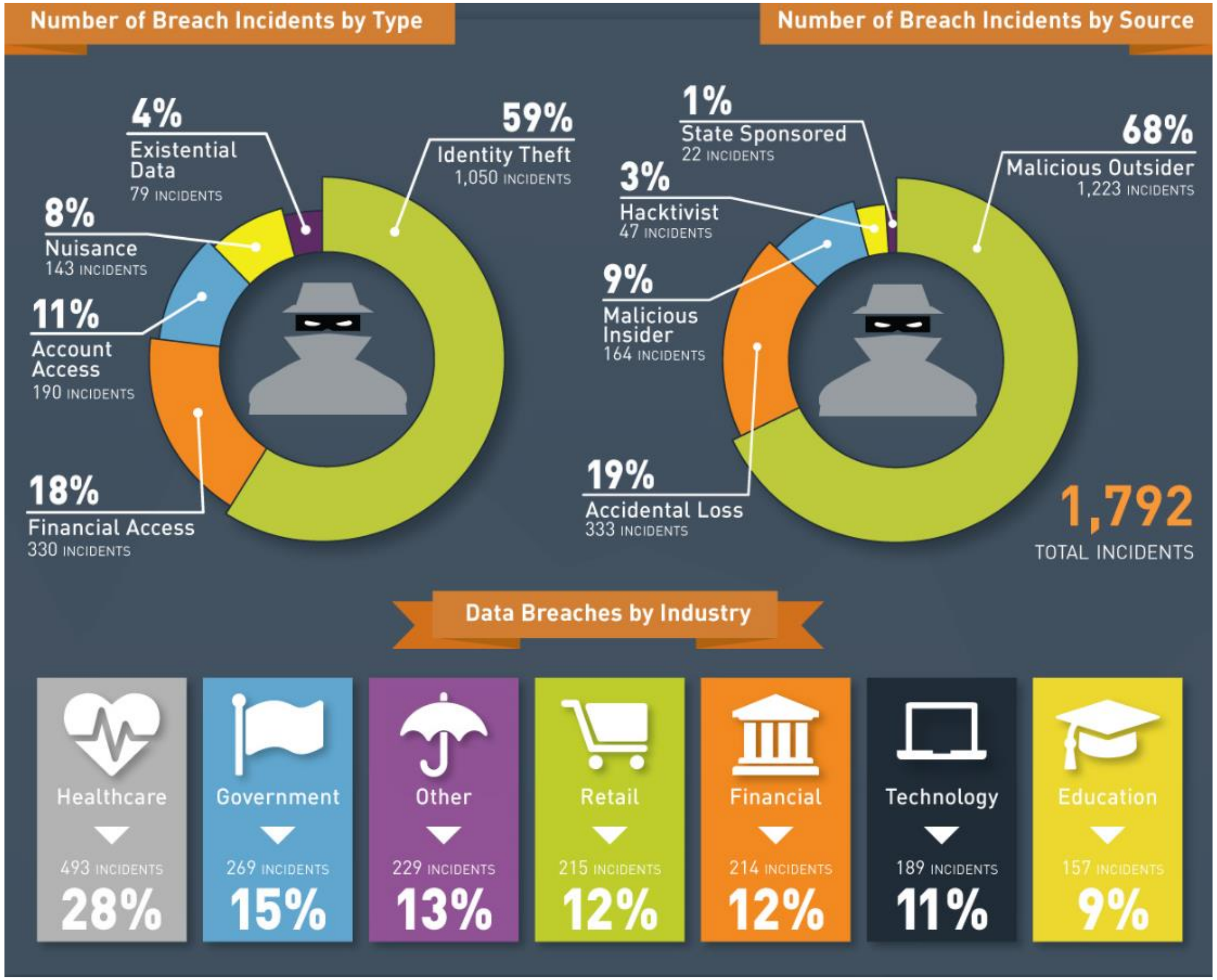
8 GLOBAL 8 INCIDENTS (<1%)

*Due to legal requirements, not all breaches are reported or publicly disclosed.
Regional differences of data may not accurately reflect total data breaches that occur.

Statistics presented are based on the Breach Level Index (breachlevelindex.com)

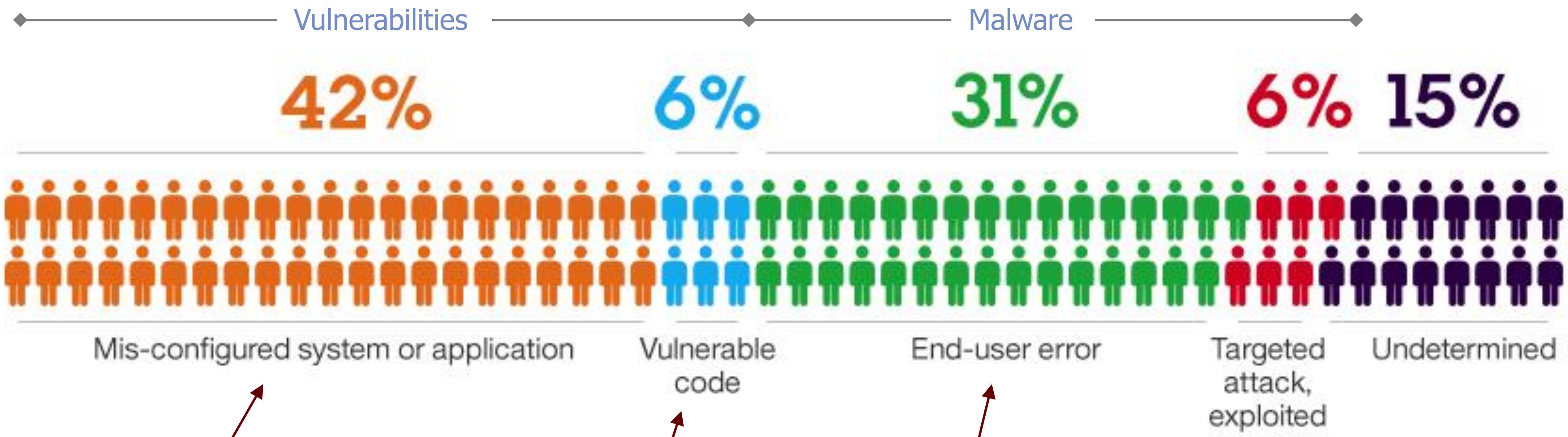
gemalto security to be free

# CYBERSECURITY BREACH BY TYPE



# CYBERSECURITY BREACH REASONS

## Why do Breaches Happen?



- Configuration Errors
- "Weak" defaults
- Easy passwords

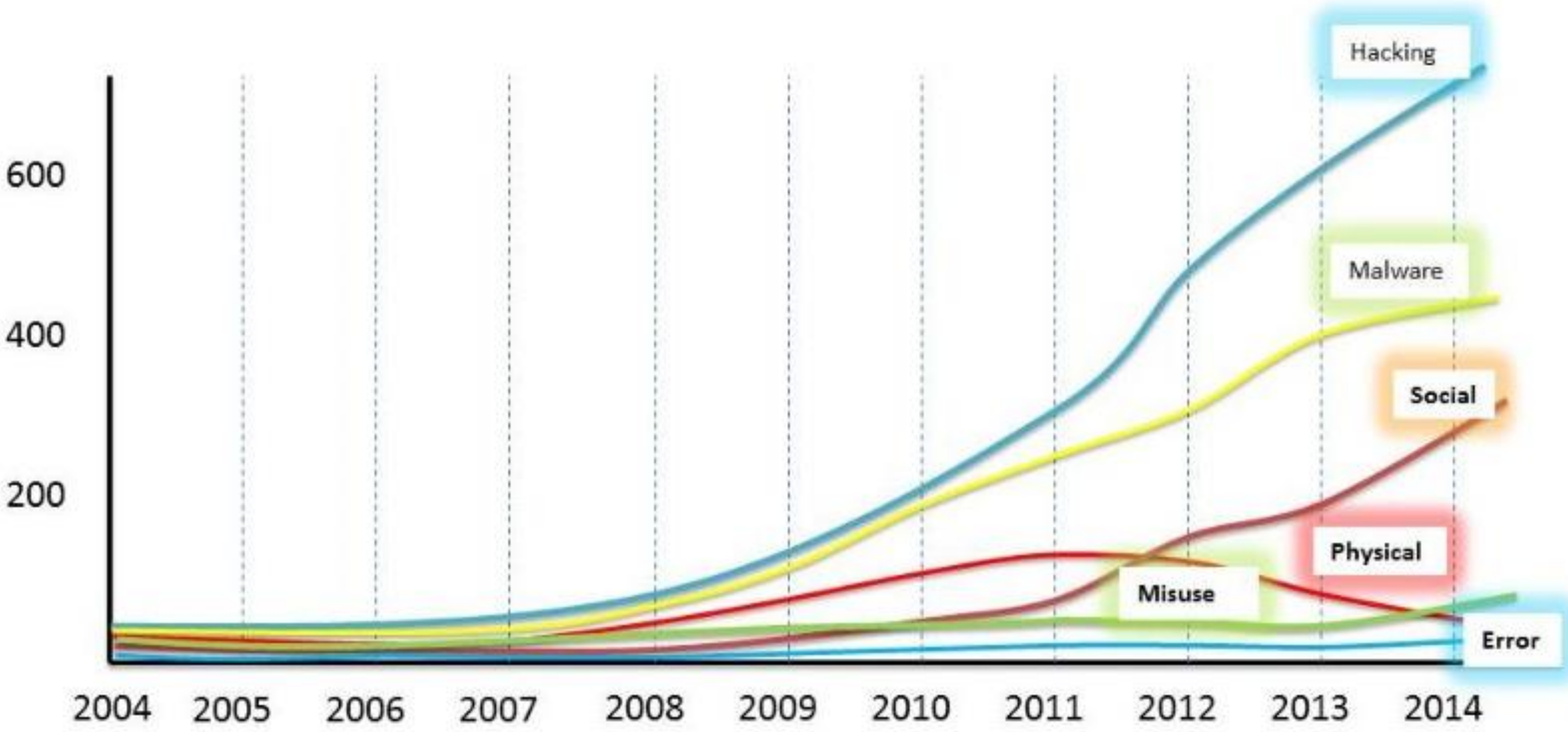
- "Bugs"
- Input validation

- Installing suspect applications
- Clicking malicious links

- Phishing Emails
- Watering Hole attacks

# CYBERSECURITY BREACH PER THREAT

Number of breaches per threat action category over time



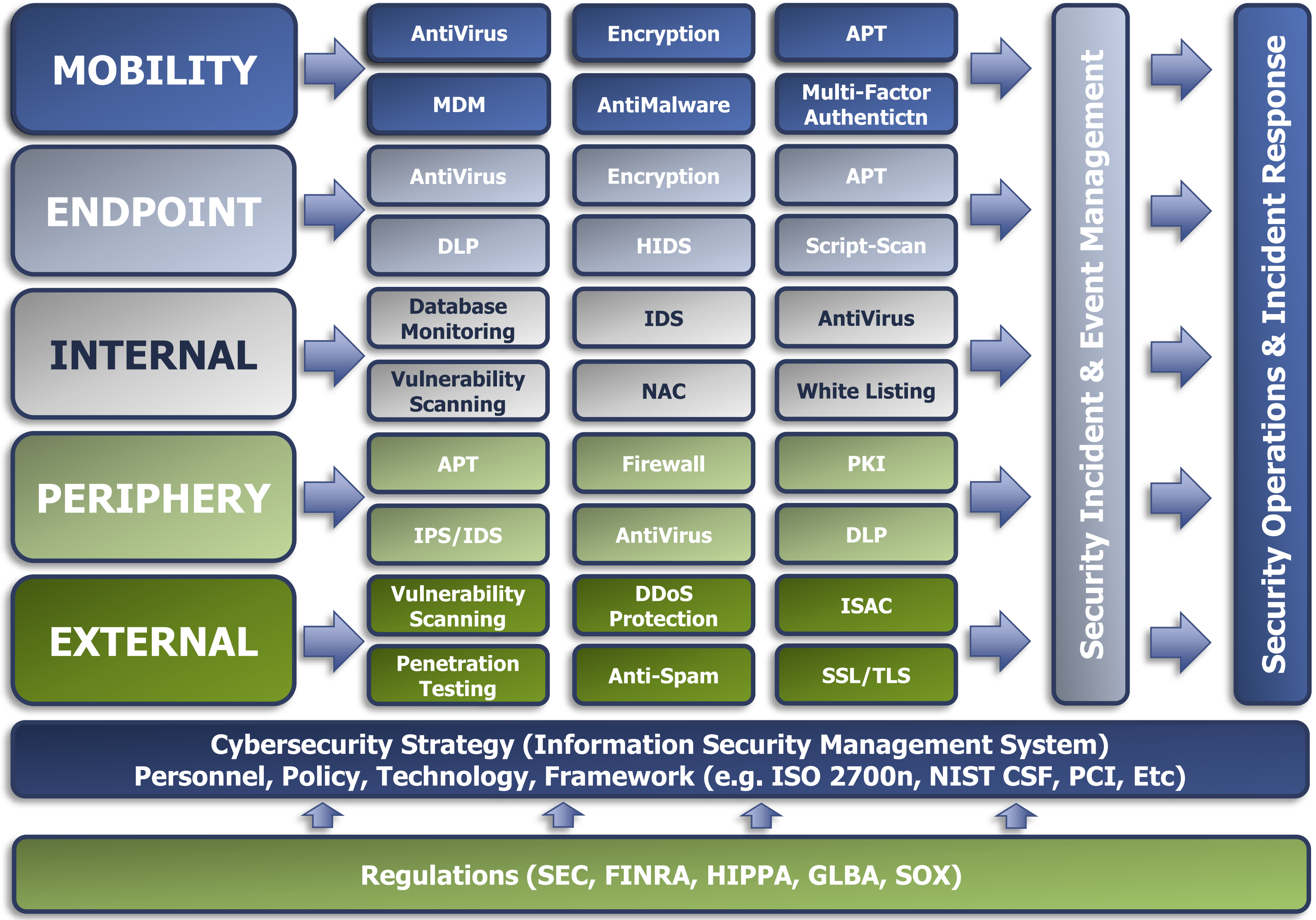
# SECURE&PROTECT STRATEGY

**Secure means Cybersecurity.**

**-Have a plan and a strategy.**

**-Regulations & compliance are pushed down from both vendors and customers.**

**-Management needs to be onboard!!!**



| | | | |
|---|---|---|---|
| MOBILITY | AntiVirus | Encryption | APT |
| | MDM | AntiMalware | Multi-Factor Authentictn |
| ENDPOINT | AntiVirus | Encryption | APT |
| | DLP | HIDS | Script-Scan |
| INTERNAL | Database Monitoring | IDS | AntiVirus |
| | Vulnerability Scanning | NAC | White Listing |
| PERIPHERY | APT | Firewall | PKI |
| | IPS/IDS | AntiVirus | DLP |
| EXTERNAL | Vulnerability Scanning | DDoS Protection | ISAC |
| | Penetration Testing | Anti-Spam | SSL/TLS |

Security Incident & Event Management

Security Operations & Incident Response

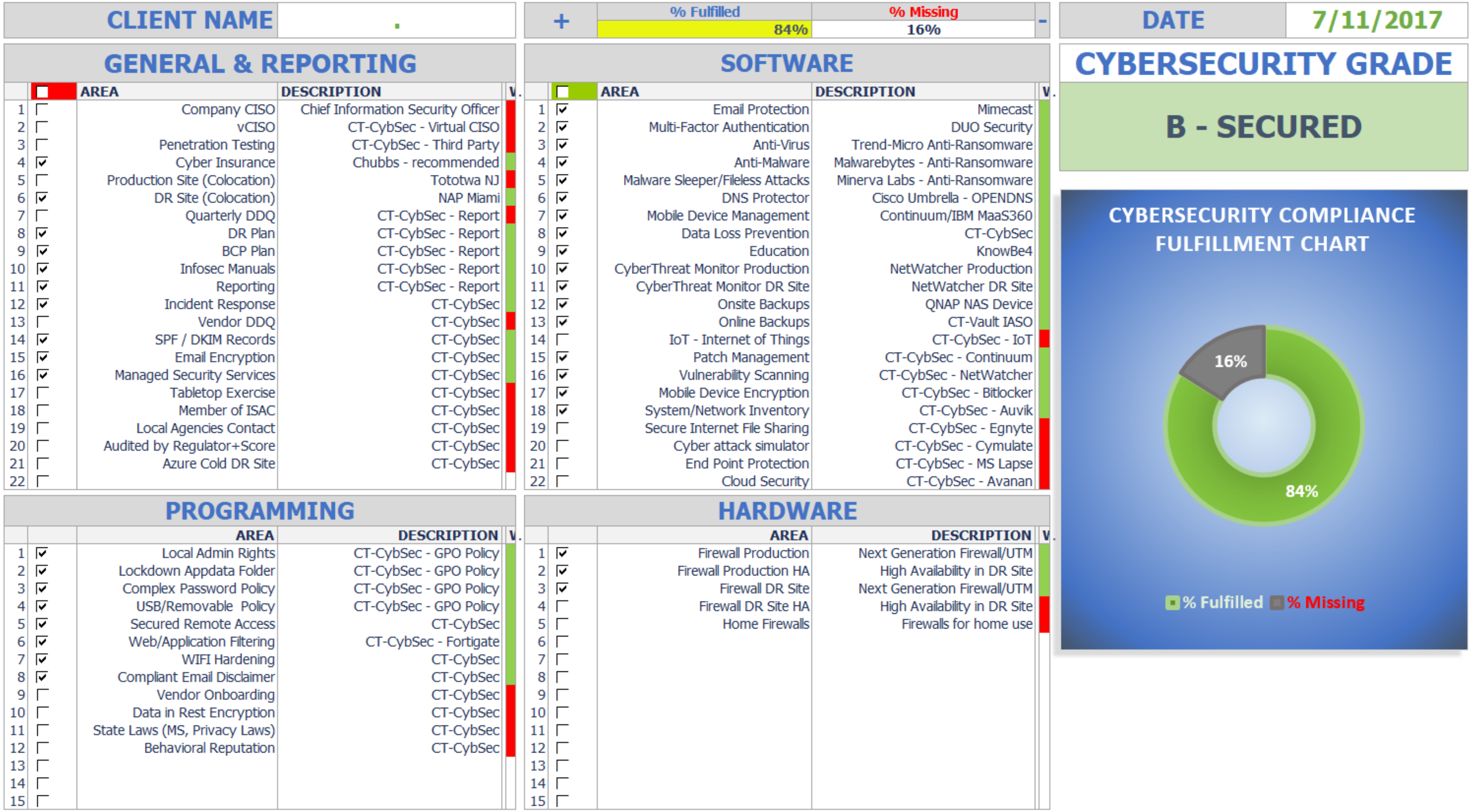
Cybersecurity Strategy (Information Security Management System)
Personnel, Policy, Technology, Framework (e.g. ISO 2700n, NIST CSF, PCI, Etc)

Regulations (SEC, FINRA, HIPPA, GLBA, SOX)

# CYBERSECURITY PARTIAL LIST

- Continuous Education
- Email Protection
- Multi-Factor Authentication
- Next Generation Firewalls
- Anti-Virus (Anti-Ransomware)
- Anti-Malware/Anti-Exploit
- Malware Sleeper (Minerva Labs)
- OpenDNS/Cisco Umbrella
- SIEM (Security Information & Event Management)
- Email Encryption
- Laptop/Smartphone Encryption
- Wireless/Firewall Hardening
- Password Vaults
- Information Security Manuals
- Security Patch Management
- Regulations & Compliance Education
- Online Backups
- Disaster Recovery Site
- Business Continuity Plan
- Incident Response
- Domain Name Spoofing Education
- Cybersecurity Insurance
- Infosec Audits
- Penetration Tests

# CYBERSECURITY GRADING SYSTEM



| CLIENT NAME | . |
|---|---|

| + | % Fulfilled | % Missing | - |
|---|---|---|---|
| | 84% | 16% | |

| DATE | 7/11/2017 |
|---|---|

## CYBERSECURITY GRADE

**B - SECURED**

## GENERAL & REPORTING

| | ☐ | AREA | DESCRIPTION | V. |
|---|---|---|---|---|
| 1 | ☐ | Company CISO | Chief Information Security Officer | 🟥 |
| 2 | ☐ | vCISO | CT-CybSec - Virtual CISO | 🟥 |
| 3 | ☐ | Penetration Testing | CT-CybSec - Third Party | 🟥 |
| 4 | ☑ | Cyber Insurance | Chubbs - recommended | 🟩 |
| 5 | ☐ | Production Site (Colocation) | Tototwa NJ | 🟥 |
| 6 | ☑ | DR Site (Colocation) | NAP Miami | 🟩 |
| 7 | ☐ | Quarterly DDQ | CT-CybSec - Report | 🟥 |
| 8 | ☑ | DR Plan | CT-CybSec - Report | 🟩 |
| 9 | ☑ | BCP Plan | CT-CybSec - Report | 🟩 |
| 10 | ☑ | Infosec Manuals | CT-CybSec - Report | 🟩 |
| 11 | ☑ | Reporting | CT-CybSec - Report | 🟩 |
| 12 | ☑ | Incident Response | CT-CybSec | 🟩 |
| 13 | ☐ | Vendor DDQ | CT-CybSec | 🟥 |
| 14 | ☑ | SPF / DKIM Records | CT-CybSec | 🟩 |
| 15 | ☑ | Email Encryption | CT-CybSec | 🟩 |
| 16 | ☑ | Managed Security Services | CT-CybSec | 🟩 |
| 17 | ☐ | Tabletop Exercise | CT-CybSec | 🟥 |
| 18 | ☐ | Member of ISAC | CT-CybSec | 🟥 |
| 19 | ☐ | Local Agencies Contact | CT-CybSec | 🟥 |
| 20 | ☐ | Audited by Regulator+Score | CT-CybSec | 🟥 |
| 21 | ☐ | Azure Cold DR Site | CT-CybSec | 🟥 |
| 22 | ☐ | | | |

## SOFTWARE

| | ☐ | AREA | DESCRIPTION | V. |
|---|---|---|---|---|
| 1 | ☑ | Email Protection | Mimecast | 🟩 |
| 2 | ☑ | Multi-Factor Authentication | DUO Security | 🟩 |
| 3 | ☑ | Anti-Virus | Trend-Micro Anti-Ransomware | 🟩 |
| 4 | ☑ | Anti-Malware | Malwarebytes - Anti-Ransomware | 🟩 |
| 5 | ☑ | Malware Sleeper/Fileless Attacks | Minerva Labs - Anti-Ransomware | 🟩 |
| 6 | ☑ | DNS Protector | Cisco Umbrella - OPENDNS | 🟩 |
| 7 | ☑ | Mobile Device Management | Continuum/IBM MaaS360 | 🟩 |
| 8 | ☑ | Data Loss Prevention | CT-CybSec | 🟩 |
| 9 | ☑ | Education | KnowBe4 | 🟩 |
| 10 | ☑ | CyberThreat Monitor Production | NetWatcher Production | 🟩 |
| 11 | ☑ | CyberThreat Monitor DR Site | NetWatcher DR Site | 🟩 |
| 12 | ☑ | Onsite Backups | QNAP NAS Device | 🟩 |
| 13 | ☑ | Online Backups | CT-Vault IASO | 🟩 |
| 14 | ☐ | IoT - Internet of Things | CT-CybSec - IoT | 🟥 |
| 15 | ☑ | Patch Management | CT-CybSec - Continuum | 🟩 |
| 16 | ☑ | Vulnerability Scanning | CT-CybSec - NetWatcher | 🟩 |
| 17 | ☑ | Mobile Device Encryption | CT-CybSec - Bitlocker | 🟩 |
| 18 | ☑ | System/Network Inventory | CT-CybSec - Auvik | 🟩 |
| 19 | ☐ | Secure Internet File Sharing | CT-CybSec - Egnyte | 🟥 |
| 20 | ☐ | Cyber attack simulator | CT-CybSec - Cymulate | 🟥 |
| 21 | ☐ | End Point Protection | CT-CybSec - MS Lapse | 🟥 |
| 22 | ☐ | Cloud Security | CT-CybSec - Avanan | 🟥 |

## CYBERSECURITY COMPLIANCE FULFILLMENT CHART

## PROGRAMMING

| | | AREA | DESCRIPTION | V. |
|---|---|---|---|---|
| 1 | ☑ | Local Admin Rights | CT-CybSec - GPO Policy | 🟩 |
| 2 | ☑ | Lockdown Appdata Folder | CT-CybSec - GPO Policy | 🟩 |
| 3 | ☑ | Complex Password Policy | CT-CybSec - GPO Policy | 🟩 |
| 4 | ☑ | USB/Removable Policy | CT-CybSec - GPO Policy | 🟩 |
| 5 | ☑ | Secured Remote Access | CT-CybSec | 🟩 |
| 6 | ☑ | Web/Application Filtering | CT-CybSec - Fortigate | 🟩 |
| 7 | ☑ | WIFI Hardening | CT-CybSec | 🟩 |
| 8 | ☑ | Compliant Email Disclaimer | CT-CybSec | 🟩 |
| 9 | ☐ | Vendor Onboarding | CT-CybSec | 🟥 |
| 10 | ☐ | Data in Rest Encryption | CT-CybSec | 🟥 |
| 11 | ☐ | State Laws (MS, Privacy Laws) | CT-CybSec | 🟥 |
| 12 | ☐ | Behavioral Reputation | CT-CybSec | 🟥 |
| 13 | ☐ | | | |
| 14 | ☐ | | | |
| 15 | ☐ | | | |

## HARDWARE

| | | AREA | DESCRIPTION | V. |
|---|---|---|---|---|
| 1 | ☑ | Firewall Production | Next Generation Firewall/UTM | 🟩 |
| 2 | ☑ | Firewall Production HA | High Availability in DR Site | 🟩 |
| 3 | ☑ | Firewall DR Site | Next Generation Firewall/UTM | 🟩 |
| 4 | ☐ | Firewall DR Site HA | High Availability in DR Site | 🟥 |
| 5 | ☐ | Home Firewalls | Firewalls for home use | 🟥 |
| 6 | ☐ | | | |
| 7 | ☐ | | | |
| 8 | ☐ | | | |
| 9 | ☐ | | | |
| 10 | ☐ | | | |
| 11 | ☐ | | | |
| 12 | ☐ | | | |
| 13 | ☐ | | | |
| 14 | ☐ | | | |
| 15 | ☐ | | | |

# QUESTIONS & ANSWERS

**Meyer Ben-Reuven**
**meyer@chelsea-tech.com**
**C - 917-251-0970**
**O-954-454-9797 / O-212-966-3355**
**www.chelsea-tech.com**