



CYBER RISK & INSURANCE

LUKE HOERR, AUSTIN KARPINSKI, KYLE VITALE, NICK
YONCE, CHRISTOPHER WEHR

WHAT WE WILL ANSWER TODAY

1. What is cyber risk?
2. What is the motivation behind cyber-attacks?
3. What kind of information can be a target?
4. What are the industry risks?
 1. Retail
 2. Manufacturing
 3. Technology
 4. Healthcare
 5. Finance

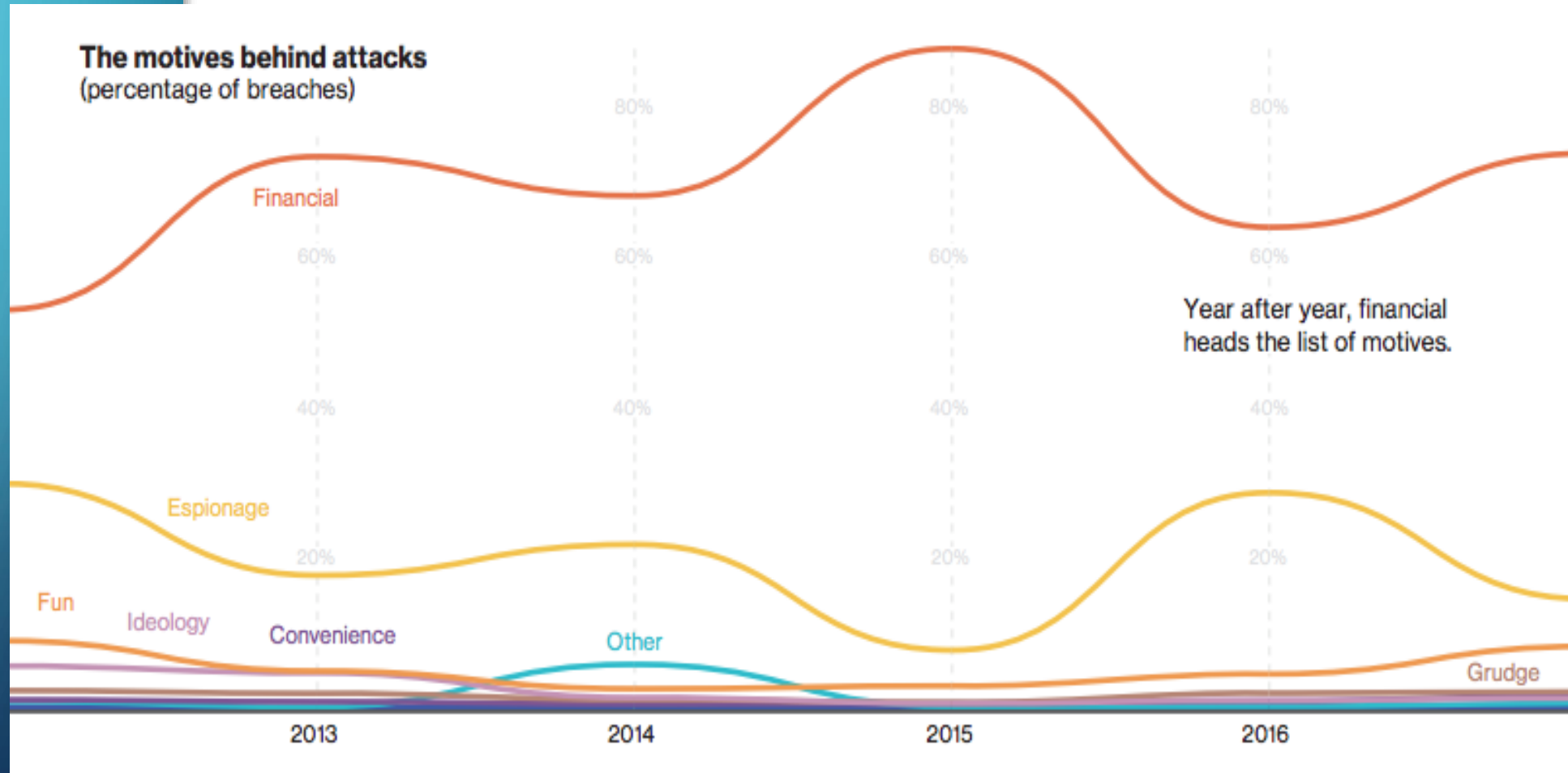
WHAT IS CYBER RISK?

'Cyber risk' means any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems.

- Financial loss
- Disruption
- Damage to reputation

MOTIVATION BEHIND CYBER ATTACKS

1. Financial
2. Espionage
3. Fun
4. Ideology
5. Convenience
6. Grudge
7. Other



INFORMATION STORED AT ORGANIZATIONS

Personally Identifiable Information (PII)

- Full name
- Date of birth
- Home address
- Gender
- Race
- Telephone number
- Social security number
- Credit card numbers
- Email address
- Biometric credentials
- Passport number
- Driver's license number
- Log in details
- Non-specific age (e.g. 30-40 instead of 32)
- Job position and workplace

Protected Health Information (PHI)

IPs, URLs/URIs

Photographic Images

Insurance Policy Numbers

Electronic Medical Record(EMR)

- Medical history
- Medications/Sedation
- Treatment plans/Medical equipment needed
- Vital signs
- Diagnosis
- Progress notes
- Immunization dates
- Allergies
- Lab/Test results

Intellectual Property (IP)

Trade secrets

Manufacturing details

Software

HOW DOES THIS INFORMATION BECOME MONETIZED?

1. Hackers create a fake identity
2. They can file fake claims and tax returns
3. They sell the information they stole on the black market
4. Ransomware encrypts patient data and demands payment in order to get the data back

RISK MITIGATION APPROACH

Insider Threat

- Employee training:
- Sending out fake simulated phishing and report. Some hospitals send out phishing emails and requiring the employees to report

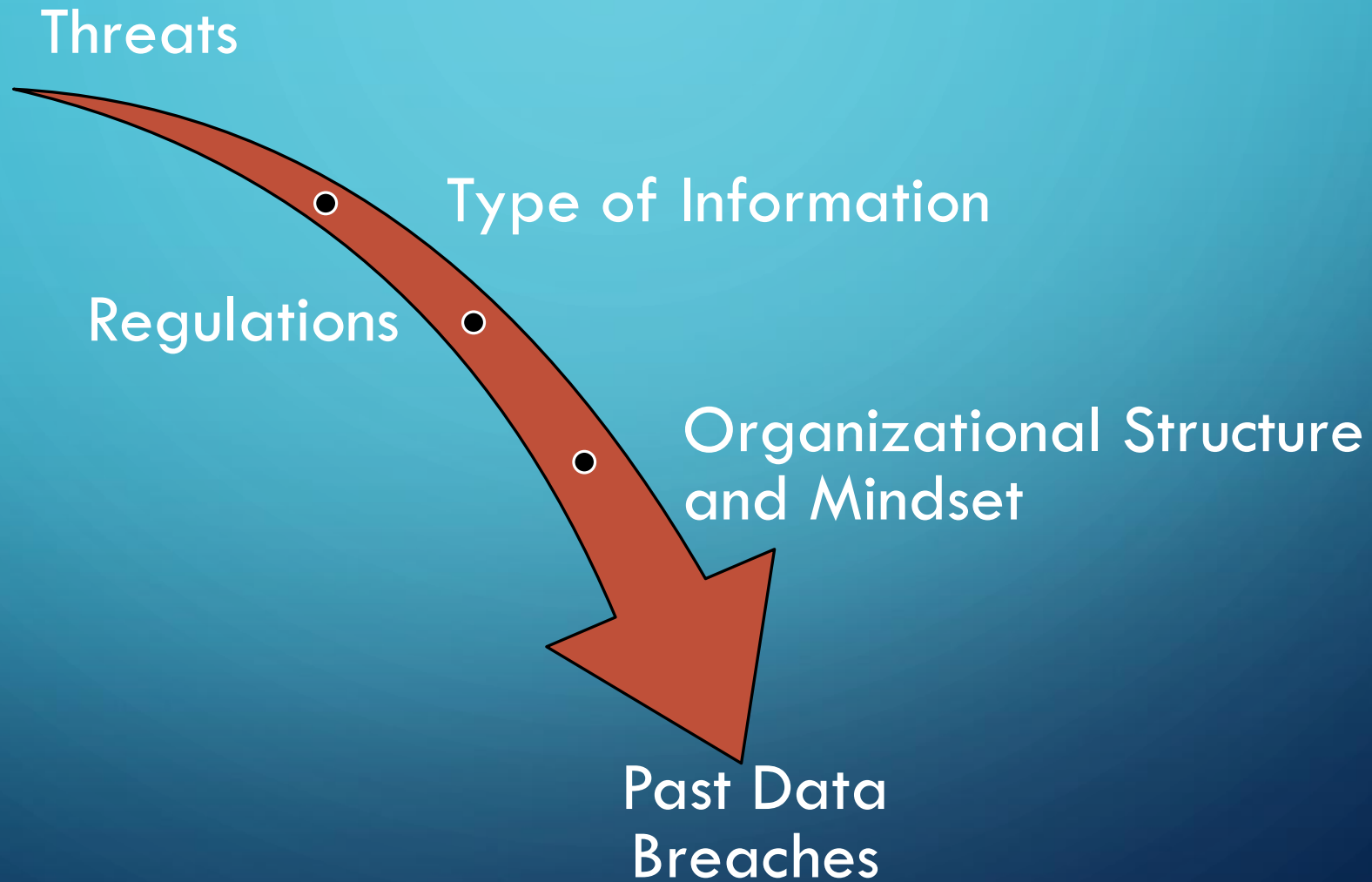
Malware

- Keep the operating system, and the network up to date
- Backup records on an external hard drive










Ensuring the company has an initiative risk management program

- Chief Information Security Officer & Chief Risk Officer

RISK ASSESSMENT MODEL FOR ALL INDUSTRIES



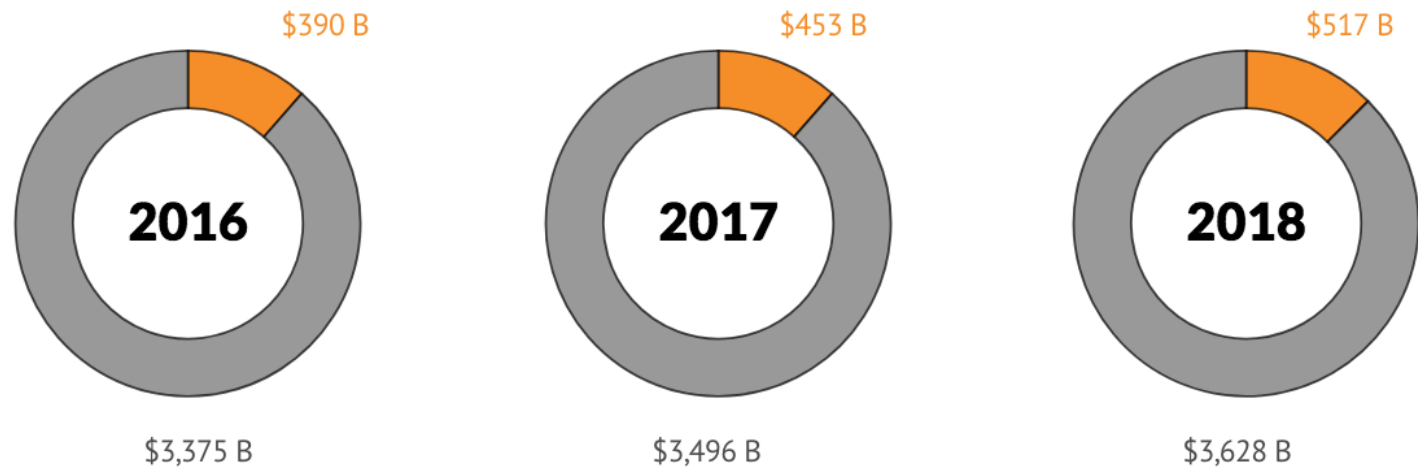
SCORING

Score	Frequency	Severity	Velocity (response time)
1-3 (Low)	Not a target 	Low amount of valuable data stored 	High quality "response" plan 
4-7 (Medium)	Somewhat targeted 	Moderate amount of valuable data stored 	Average "response" plan 
8-10 (High)	Constantly targeted 	High amount of valuable data stored 	No focus on action plan 

RETAIL

- Ecommerce represented 14.3% of total retail sales in 2018
- Retailers collect data about their customer
 - Personal information
 - Financial information
 - Behavior

U.S. **ECOMMERCE** VS. TOTAL RETAIL SALES



Digital Commerce 360: US ecommerce sales grow 15.0% in 2018

COMPANY COMPARISON



- Hacking and business disruption
- PII
- PCI & as an international company exposed to different national regulation

Frequency: 5 | Severity: 4 | Velocity: 5 |

Overall: 100



- Hacking and business disruption
- PII & PHI
- HIPAA & PCI

Frequency: 6 | Severity: 8 | Velocity: 6 | Overall: 252

MANUFACTURING

- Top cyber liabilities- data breaches, stealing of intellectual property, third party damages, business interruption, and cyber extortion
- Current software used in the manufacturing industry has weak security
- The Manufacturing industry is second most attacked industry behind healthcare

MAJOR THREATS

- When it comes to manufacturing, Intellectual property is the most valuable asset
- "The largest risk would be cybercriminals attempting to steal intellectual property and trade secrets NCMS says 21% of manufacturers have lost intellectual property and 90% of the data stolen is considered proprietary"
 - Team, Barkly. "Cyber Attacks Against Manufactures on the Ris
- An alteration in the manufacturing process could cause huge recalls, and possible compromised products
- Locking out the manufacturer from their Manufacturing Operation System (MOS)
 - Recent occurrence

COMPANY COMPARISON



- Use Amazon cloud computing for their cloud storage
- In February 2018 their cloud was hacked but no data was leaked
- Only manufactures in California, Nevada, and Buffalo New York
- Tesla created their own MOS or Manufacturing operations software
 - This is unique as most of the time companies will buy one and have it modified for their needs

• **Frequency: 5 | Severity: 6 | Velocity: 8 | Overall: 240**

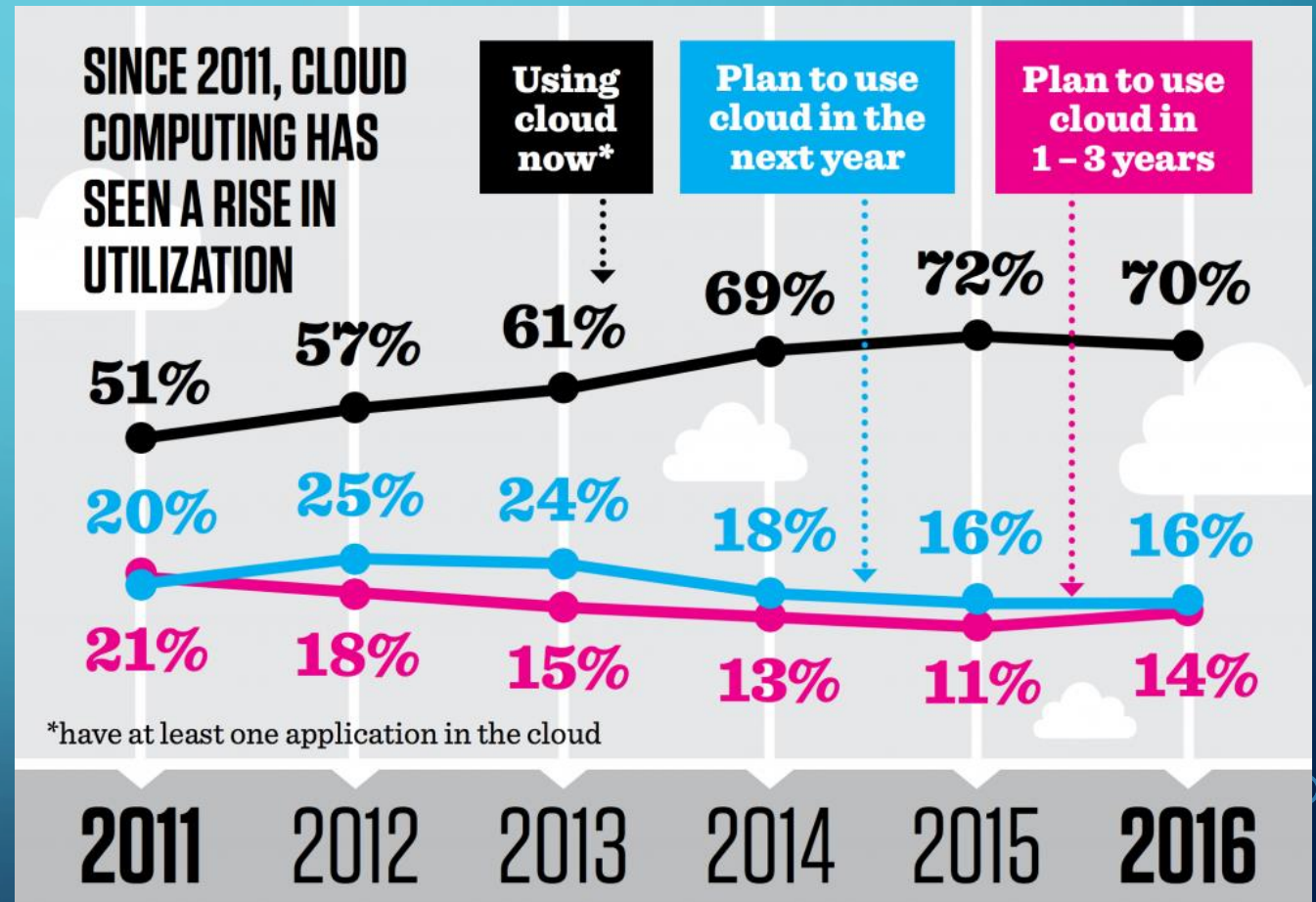


- EMC is a recent acquisition with dell, and is a cloud computing company and manages all their own in-house cloud storage
- Would have PII for employees, customers, and possible clients on cloud computing platform EMC
- Had an attempted hack in November 2018, but its website uses (Hashing) to scramble passwords and nothing was stolen.
 - Has manufacturing plants scattered all over the world

Frequency: 3 | Severity: 4 | Velocity: 6 | Overall: 72

TECHNOLOGY – RISE OF CLOUD COMPUTING

- 81 percent of enterprises have a multi-cloud strategy
- Cloud companies prioritize efficiency over security
- Cloud Security Alliance identified data breaches as the largest of 12 threats



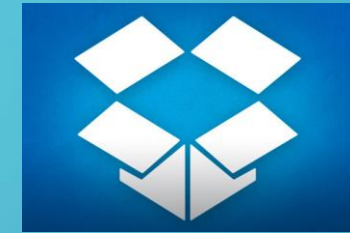
CLOUD COMPUTING'S IMPACT ON CYBER INSURANCE

- As companies shift from internal storage of data to external storage, the importance of third-party coverage rises drastically
- Chinese hackers "APT 10" breached a U.S. IT firm, gaining access to 45 companies in 12 countries, and the U.S. Navy
- Cyber insurance companies must take advantage of this strategic window by focusing on cloud companies that prioritize security

COMPANY COMPARISON



salesforce



Dropbox

- Most widely used CRM tool in the world
- Offers in house security bundle "Shield" and external security through cloud security broker
- Acquired data encryption firm Navajo Systems
- Warned of possible breach in 2018 of marketing platform allowing other customers to view data

Frequency: 4 | Severity: 8 |
Velocity: 5 | Overall: 160

- Most popular cloud storage/file sharing system
- 95% of cloud security failures will be the customers' fault
- Massive breach in 2011, revealing 68 million users login info
- Launched Dropbox Business following breach with extra security features

Frequency: 6 | Severity: 7 |
Velocity: 7 | Overall: 294

HEALTHCARE

- Top Threats: Ransomware, Insider Threat.
- Description of trends: Significant change is expected to be coming to the healthcare industries information systems and functionality.
- Type of info at risk: credit cards, social security numbers, employment info., medical history, (all this is used to create medical identities)
- Average cost of a Medical Record : \$408



COMPANY COMPARISON



NORTH WESTERN MEMORIAL

- June 2012
 - Stolen computers: software update exposure
 - At Least 500 individuals
 - Hospital contended that the PHI was not the target of attack
- March 2019
 - Insider Threat
 - 60 employees fired for accessing Jussie Smollett's Medical Record

Frequency: 7 | Severity: 8 | Velocity: 6 |

Overall: 366

JOHNS HOPKINS HOSPITAL

- June 2017
 - Network Hack
 - Employee data exposed
 - Affected nearly 3.8 million identified members
 - Member's name, mailing address, type of plan, member and group ID number, names of dependents enrolled in the plan, primary care provider and, for some companies, date of birth, premium invoice information and Medicaid ID number.

Frequency: 8 | Severity: 9 | Velocity: 7 |

Overall: 504

FINANCIAL

Top Threats

- Third-, fourth- and fifth-party vendors
 - Harder to secure from a risk standpoint
- Web application attacks
 - “The threat of cyber security may very well be the biggest threat to the U.S. financial system,” - Jamie Dimon CEO of JP Morgan Chase
- Talent shortage/ mismanagement
 - Chief information security officer reporting to CEO not CIO/CRO
- Large range of products offered by companies in this space
 - Data becomes decentralized quickly

RISK PROFILE LEVEL

LOW RISK PROFILE

- Larger multinational corporations
- Established risk management program
- Strong accountability at the executive level

HIGH RISK PROFILE

- Smaller "regional" corporations
- Lots of third-party risks
- Doesn't seek adequate insurance
- Has a fully centralized cybersecurity program

COMPANY COMPARISON



JPMORGAN CHASE & CO.

- New York City, NY
- Over 250,000 employees
- 2.6+ trillion in assets
- Core competency: commercial banking, retail financial services
- Follows NYDFS Regulations
- Breach affecting 76M in 2014

Frequency: 4 | Severity: 9 | Velocity: 6 |
Overall: 216



AMERICAN
EXPRESS

- New York City, NY
- Over 55,000 employees
- 181+ billion assets
- Core competency: charge cards, credit cards
- Follows NYDFS Regulations
- 3rd party breach affecting 700k in 2018 (India)

Frequency: 3 | Severity: 8 | Velocity: 6 |
Overall: 144

CONCLUSION

	Organization	Frequency	Severity	Velocity	Overall
Retail	Best Buy	5	4	5	100
	CVS Pharmacy	6	8	6	288
Manufacturing	Tesla	5	6	8	240
	Dell	3	4	6	72
Technology	Salesforce	4	8	5	160
	Dropbox	6	7	7	294
Healthcare	Northwestern	7	8	8	366
	John Hopkins	8	9	7	504
Finance	American Express	3	8	6	144
	JP Morgan Chase	4	9	6	216