Supplier Cyber Regulatory Awareness

Legal Issues in Cybersecurity

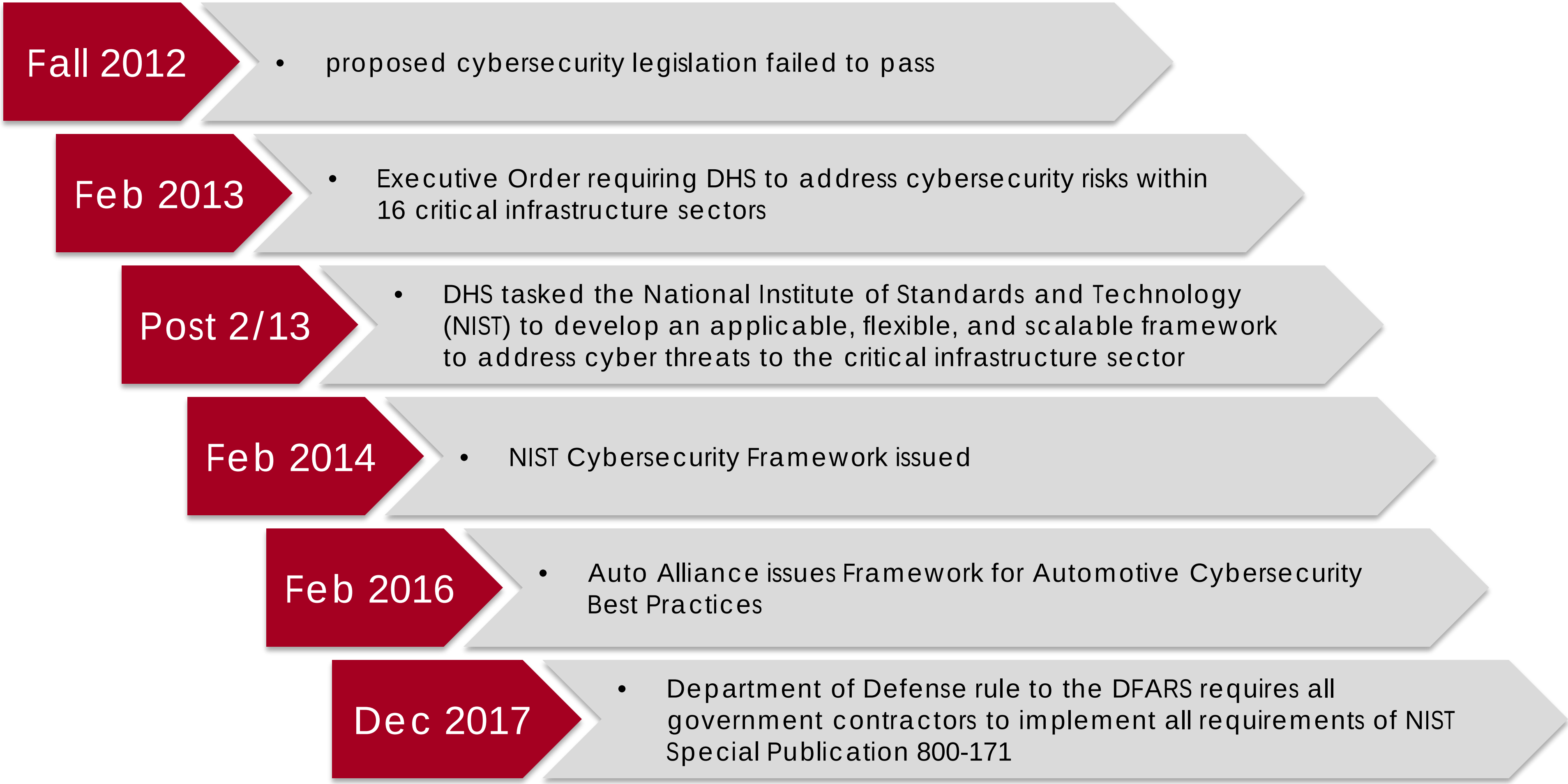
September 27, 2017

BUTZEL
LONG

Claudia Rast | Butzel Long | Ann Arbor, MI | rast@butzel.com

FACTS, STATISTICS & RISKS

Cybersecurity 101



Fall 2012

- proposed cybersecurity legislation failed to pass

Feb 2013

- Executive Order requiring DHS to address cybersecurity risks within 16 critical infrastructure sectors

Post 2/13

- DHS tasked the National Institute of Standards and Technology (NIST) to develop an applicable, flexible, and scalable framework to address cyber threats to the critical infrastructure sector

Feb 2014

- NIST Cybersecurity Framework issued

Feb 2016

- Auto Alliance issues Framework for Automotive Cybersecurity Best Practices

Dec 2017

- Department of Defense rule to the DFARS requires all government contractors to implement all requirements of NIST Special Publication 800-171

Current Federal Standard: NIST

NIST Cybersecurity Framework:

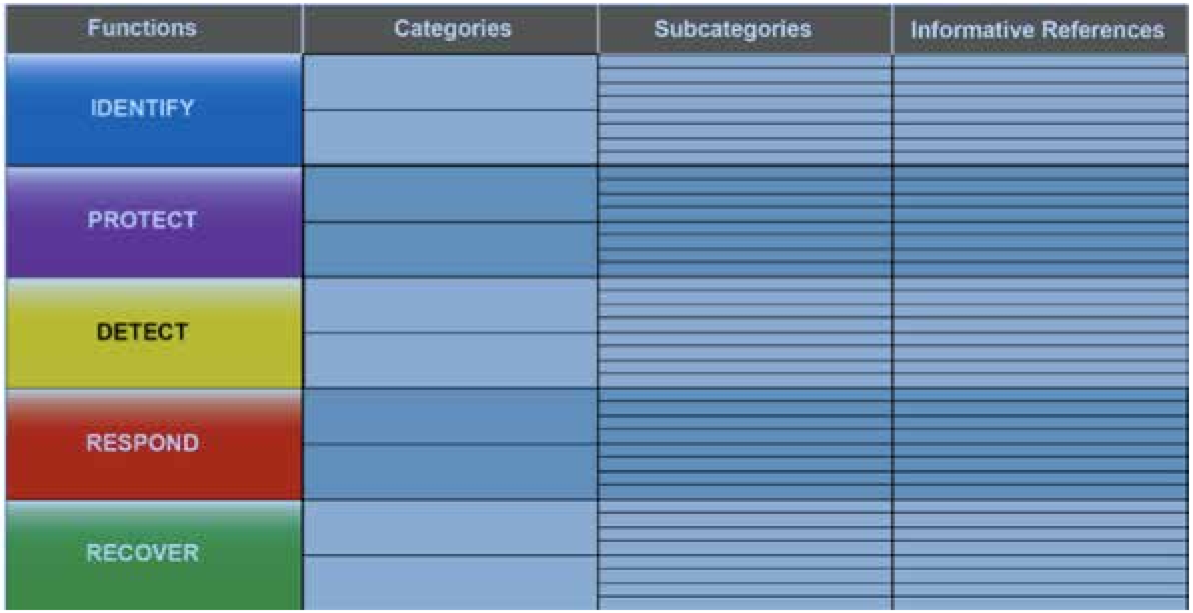
Identify

Protect

Detect

Respond

Recover



Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Breach Costs & Risk Protection

- Technology breaches are more expensive than most (+$21 per record)
- Companies with Incident Response Plan in place pay $19 less per compromised record
- Encryption reduces the cost by $16
- Employee training reduces the cost by $12.50
- Companies who alerted customers too soon pay $5.50 more per compromised record
- Average time to identify a breach: 191 Days

Nine Common Patterns

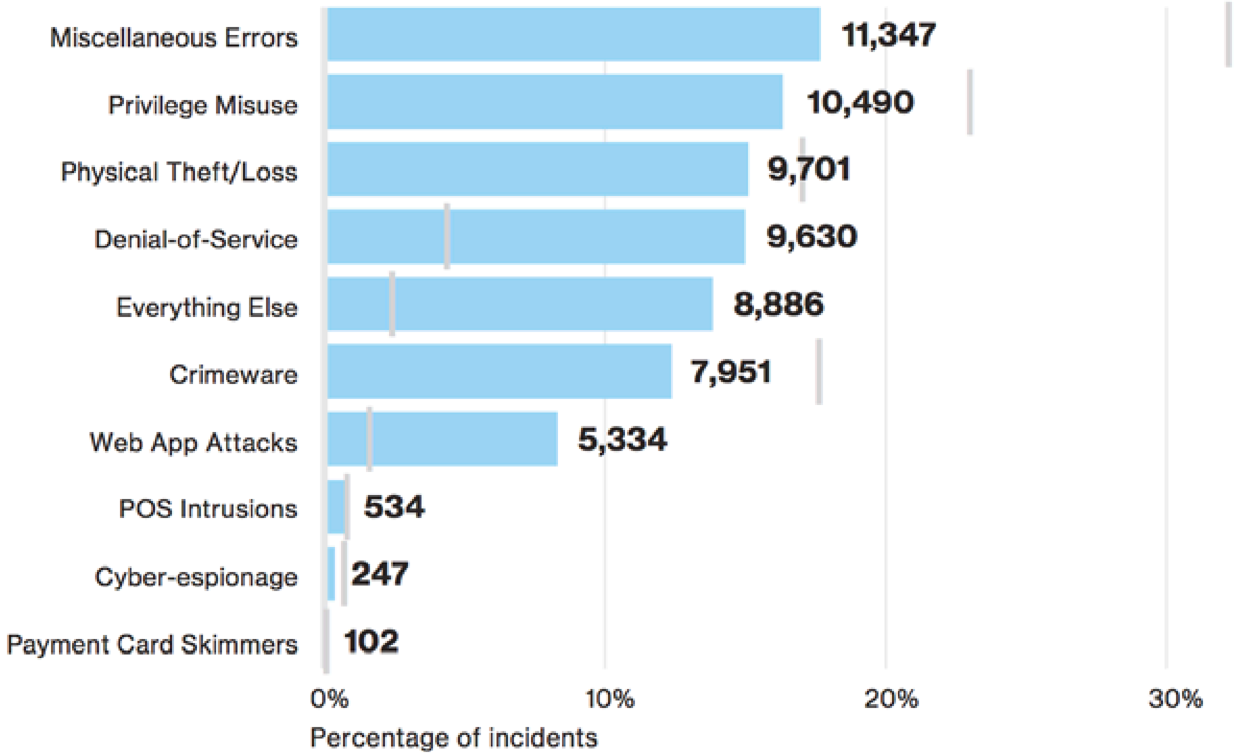


Figure 17.

Percentage (blue bar), and count of incidents per pattern. The gray line represents the percentage of incidents from the 2015 DBIR. (n=64,199)

Source: 2016 Verizon Data Breach Investigation Report

Who Are They?

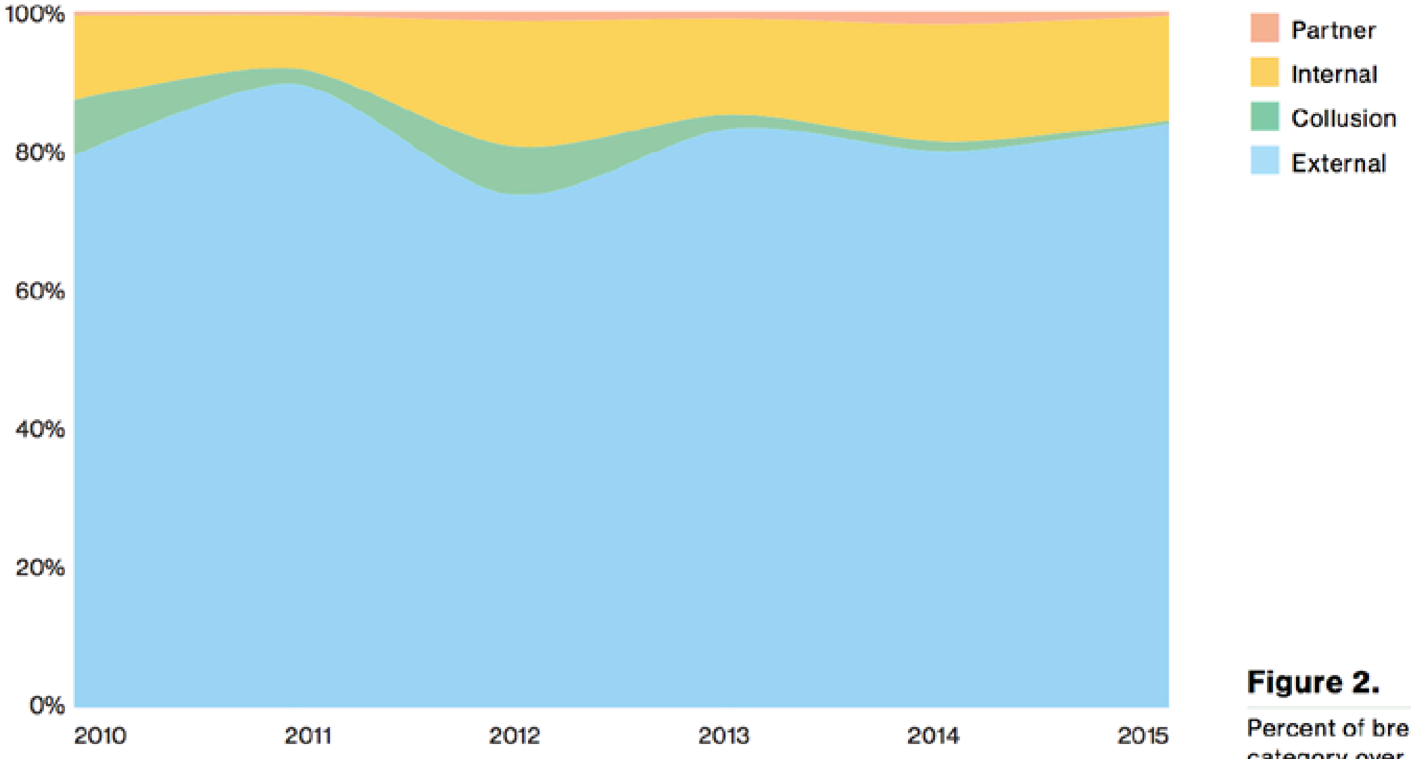


Figure 2.

Percent of breaches per threat actor category over time, (n=8,158)

Source: Verizon 2016 Data Breach Investigations Report, 4/29/16

What Are Their Weapons?

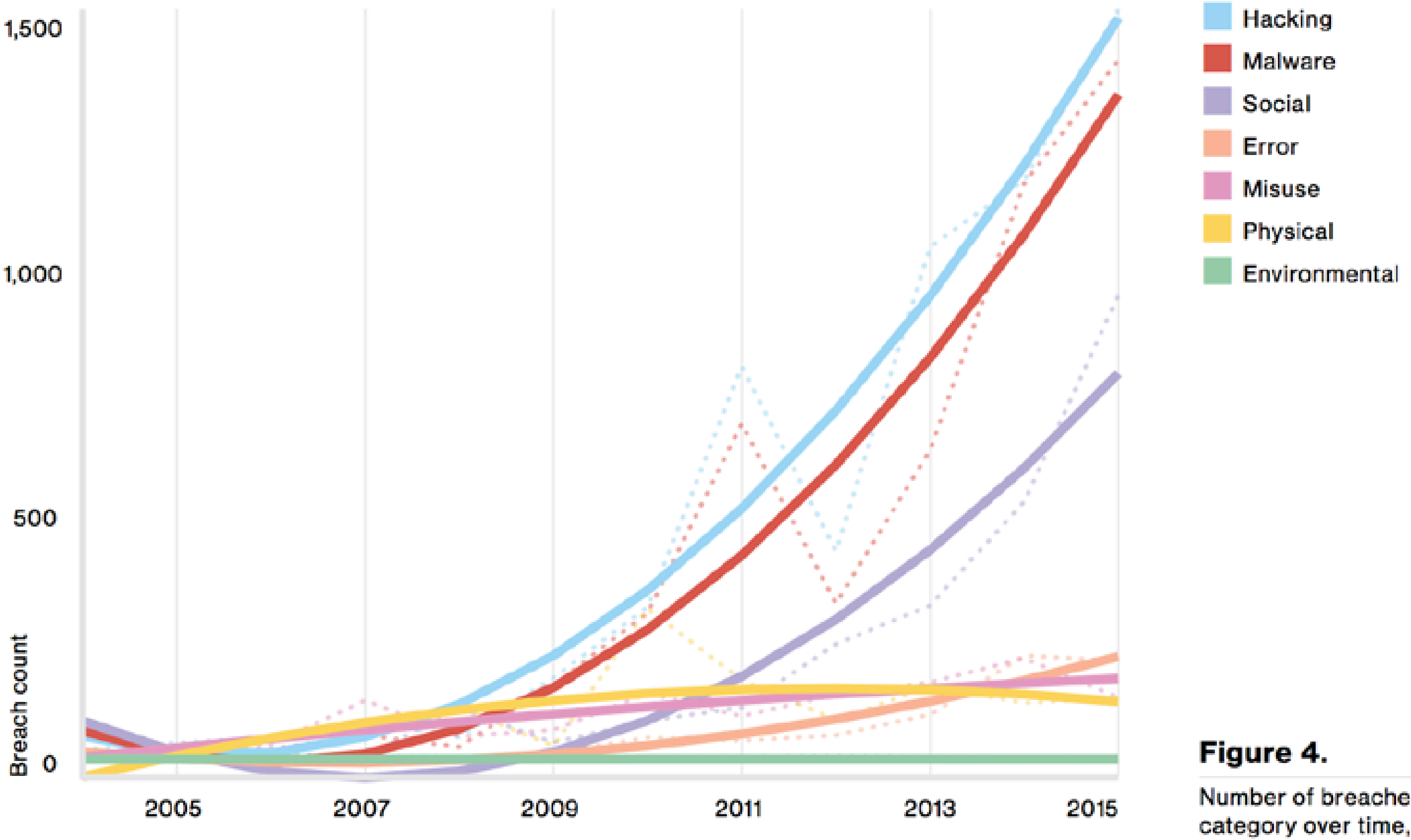


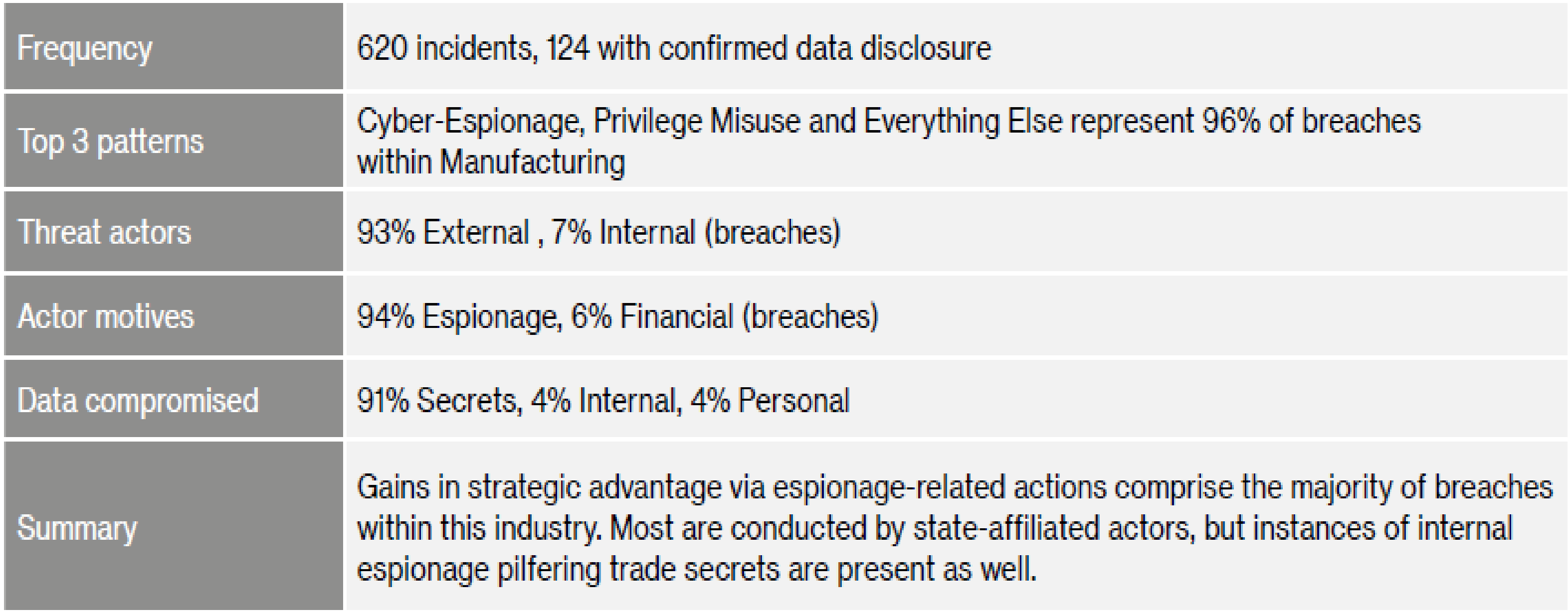
Figure 4.

Number of breaches per threat action category over time, (n=9,009)

Source: Verizon 2016 Data Breach Investigations Report, 4/29/16

Cyber Incidents: Manufacturing

Verizon 2017 Data Breach Investigations Report



Frequency	620 incidents, 124 with confirmed data disclosure
Top 3 patterns	Cyber-Espionage, Privilege Misuse and Everything Else represent 96% of breaches within Manufacturing
Threat actors	93% External , 7% Internal (breaches)
Actor motives	94% Espionage, 6% Financial (breaches)
Data compromised	91% Secrets, 4% Internal, 4% Personal
Summary	Gains in strategic advantage via espionage-related actions comprise the majority of breaches within this industry. Most are conducted by state-affiliated actors, but instances of internal espionage pilfering trade secrets are present as well.

Predominant Breach?

- Cyber-espionage!
  - From the 2107 Verizon DBIR

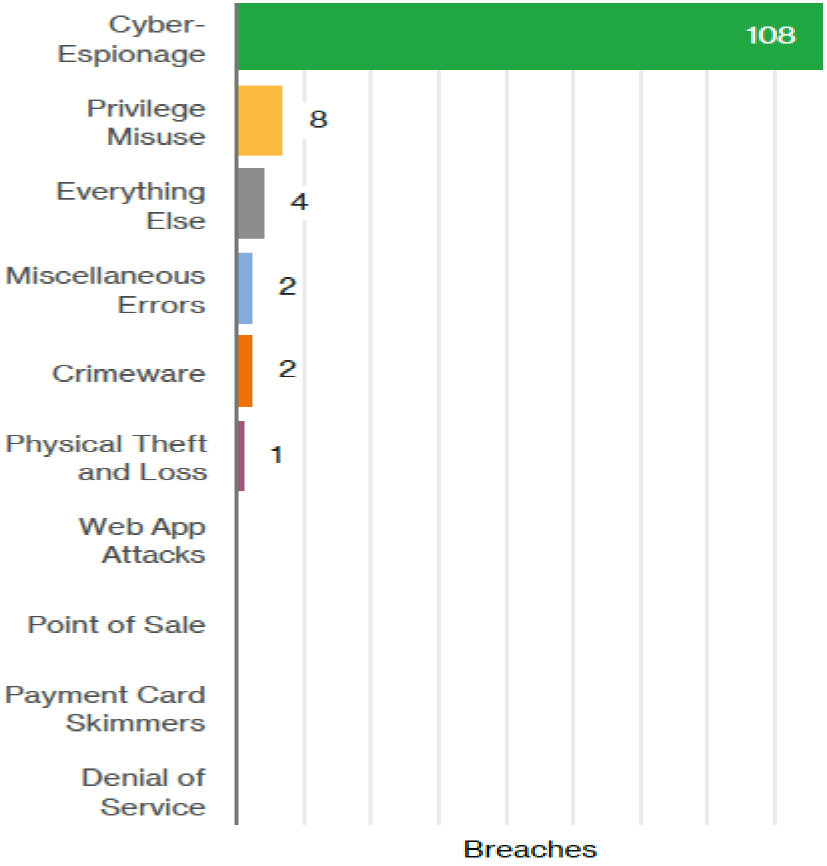


Figure 24: Frequency of incident classification patterns within Manufacturing industry breaches (n=124)

KNOW THE RISKS—RESPOND WITH TERMS

NIST SP 800.171

- December 30, 2015: DoD published its interim rule to the Defense Acquisition Federal Regulation Supplement (DFARS) giving gov't contractors until December 31, 2017, to implement NIST SP 800.171
- Failure to meet the requirement à loss of contracts
- NIST 800.171 is a subset of NIST 800.53

DFARS CDI/CUI Compliance

- Are you a DoD Government Contractor?
- Does your company work with CDI/CUI?
- Is DFARS clause 252.204.7008 in your Contract?
- If yes to the above, then you have 30 days to complete a DFARS CDI Assessment & report to the DoD CIO upon contract award

What Laws or Regulations Apply?

- Criminal Code—Title 18
  - Computer Fraud & Abuse Act, 18 U.S.C. § 1030
  - Wiretap Act, 18 U.S.C. § 2511
  - Stored Communications Act (unlawful access), 18 U.S.C. § 2701
  - Identity Theft, 18 U.S.C. § 1028(a)(7) & § 1028A
  - Electronic Communications Privacy Act, 18 U.S.C. § § 2510-2522
  - Economic Espionage Act, 18 U.S.C. § § 1831-1839
- Other Federal Law & Regulations: HIPAA/HITECH (Healthcare), FTC Act (Online Commerce), GLB & OCC (Financial), Federal Privacy Act (Gov't), FIPS 199 & 200
- State Data Breach Laws (48 states plus DC, Puerto Rico, Virgin Islands)
- ISO 26262 / SAE J3061 (Auto Manufacturing)

Common DFARS Clauses

- 252.204.7008 – Compliance with Safeguarding Covered Defense Information Controls
- 252.204.7009 – Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information
- 252.204.7012 – Safeguarding Covered Defense Information and Cyber Incident Reporting

What is CDI/CUI?

- Any unclassified information provided by or on behalf of DoD in connection with the contract or collected, developed, received, transmitted, used, or stored by or on behalf of the contractor under the contract, such as:
  - Controlled technical information
  - Critical information (operations security)
  - Export control
  - Any other information, marked or identified in the contract requiring security controls pursuant to and consistent with applicable law and Government-wide policies (e.g., privacy, proprietary business information)

Performing the GAP Analysis

- While there are hundreds of “controls,” you only need to map to legitimate concerns
- The Goal: Protecting Covered Defense Information (CDI) or Controlled Unclassified Information (CUI) or Unclassified Controlled Technical Information (UTCI)

The Family of Controls

1. Access Control
2. Audit and Accountability
3. Awareness and Training
4. Configuration Management
5. Identification and Authentication
6. Incident Response
7. Maintenance
8. Media Protection
9. Physical Protection
10. Personnel Security
11. Risk Assessment
12. Security Assessment
13. System and Communications Protection
14. System and Information Integrity

Terms to Review

- Security/Privacy Representations
- What type of Data
- Compliance with Laws (US, EU, UK?)
  - Privacy Shield/GDPR
- Indemnification
- Insurance (Cyber Liability Coverage)
- Server Locations
  - In state? Out of state? Out of the country?
- Cloud Provider? (FedRAMP: https://www.fedramp.gov/)
- Security protocols for breach notification

Cyber Liability Insurance

- Data Breach: Failure to protect an individual's privacy – 1st Party Costs , Notification, Forensics, Legal Assistance, Credit Monitoring, PR Firms.
- Data Breach: Failure to protect an individual's privacy – 3rd Party Costs, Defense Costs & Settlements
- Network Security: Loss or damage to a network & data, 1st & 3rd Party (may include lost income)
- Media Liability: Web content (Libel, Defamation)
- Fines & Penalties (HIPAA, PCI)
- eVandalism & Extortion
- Property loss from Cyber Perils (Internet of Things)

We’ve Been.... Breached

- Call your Cybersecurity Counsel first
  - Do NOT let your internal IT “fix” the problem
  - Do NOT call the police or FBI before calling counsel
  - Consider the breach to be a crime scene needing yellow “tape”
- Pull out your incident response plan.
- Don’t act before investigating and assembling your team.
- Initiate the notification process as needed ***and as required by law***
- ***You may be surprised at what you discover with thorough forensic examination***

WHAT SHOULD MANAGEMENT AND/OR THE BOARD OF DIRECTORS DO?

Corporate Board Liability

There is increasing importance for corporate boards to take responsibility for cybersecurity issues

DO THIS: **Appoint a CISO that reports directly to the Board**

SEC Commissioner: boards are a critical part of risk management in cybersecurity (perhaps ironic?)

FINRA and FTC have an interest in boards working to mitigate security risks (FTC investigation of Equifax)

NIST finds board involvement critical to successful implementation of the framework

Five Principles for Management & Board of Directors

1. Approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue
2. Understand the legal implications of cyber risks related to company's specific circumstances
3. Adequate access to cybersecurity expertise and regular discussions at meetings
4. Set expectations for management/staff and provide staff and budget
5. Review of risk assessment

Source: NACD Cyber-Security Oversight Handbook

Questions Management & Board Should Ask

1. Does the organization use a security framework?
2. What are the top five risks the organization has related to cybersecurity?
3. How are employees made aware of their role related to cybersecurity?
4. Are external and internal threats considered when planning cybersecurity program activities?
5. How is security governance managed within the organization?
6. In the event of a serious breach, has management developed a robust response protocol?

Source: IIARF Research Report (IIA-ISACA)

BEST PRACTICES

Best Practices for Individuals

- Set **Browser Security** to Standard established by IT
- Do not Borrow a **flash drive** from someone you don't know; if you're unsure, have IT scan it
- Never share **passwords**
- Do not click on **links from untrusted sources**—if you're unsure, forward to IT
- If an **email seems suspicious**, call the sender; always double-check before sending any sensitive data
- **BYOD**—cell phones, iPads, tablets, etc. implement security; mobile device management (remote wipe)

Best Practices for Management

- Perform Risk Assessment (Physical Plant, Information Systems & Workforce)
- Segregate & Secure High Risk Information, Operations & Workers
- Encrypt Sensitive Data/Implement Robust Password Policy
- Implement Company-wide Training (Ongoing)
- Incorporate Security By Design (i.e., from the beginning)

Best Practices for Management

- Acquire Cyber Liability Insurance
- Enable Network Security Monitoring & Review of Log Files (Lesson Learned from Target)
- Demand Compliance from Contractors & Suppliers (Another Lesson from Target)
- Conduct Table-Top Drills
- Have Experts at the Ready If/When an Attack Occurs

Best Practices for IT Departments

- Eliminate Unnecessary Data
- Conduct Ongoing & Active Risk Analysis
  - Vulnerability testing (external & internal)
- Collect, Analyze & Share Incident Data
- Collect, Analyze & Share Tactical Threat Intelligence, Especially Indicators of Compromise
- Focus on Better & Faster Detection
  - Log files & monitoring post CISA

Best Practices for IT Departments

- Use Metrics to Drive Security – Unusual Activity?
- Evaluate Threat Landscape to Prioritize Treatment Strategy
- Track Workforce: Who’s Who, What they Do & When they Go
- TEST Backups
- Encrypt
- Two-factor authentication
- Patch, upgrade & update

Best Practices Overall

- Know **What** Data You Have and **Where** you Store It
- Perform **Risk Assessment** (Physical Plant, IT Systems & Workforce)
- **Segregate** & **Secure High Risk Information**
- **Encrypt** Sensitive Data/Implement Robust Password Policy
- Implement Company-wide **Training** (Ongoing)
- Cyber Liability **Insurance**
- **Enable Network Security** Monitoring & Review of Log Files
- Demand **Vendor Compliance**: Remember Target?
- Conduct Table-Top **Drills**
- Have **Experts at the Ready** If/When an Attack Occurs

Thank You!

Claudia Rast | Butzel Long | Ann Arbor, MI | rast@butzel.com