Cybersecurity: An Ounce of Prevention and Governance are Worth a Pound of Cure

Brandon Pattison, Corporate Attorney, Arrow Electronics
Lucky Vidmar, Technology Counsel, Western Union
Helena Ledic, Associate General Counsel, CSC

January 16, 2020

Introductions and Speakers

Brandon Pattison
Corporate Attorney
Arrow Electronics

Lucky Vidmar
Vice President & Senior Counsel
Head of Technology, IP, Procurement & Real Estate
Western Union

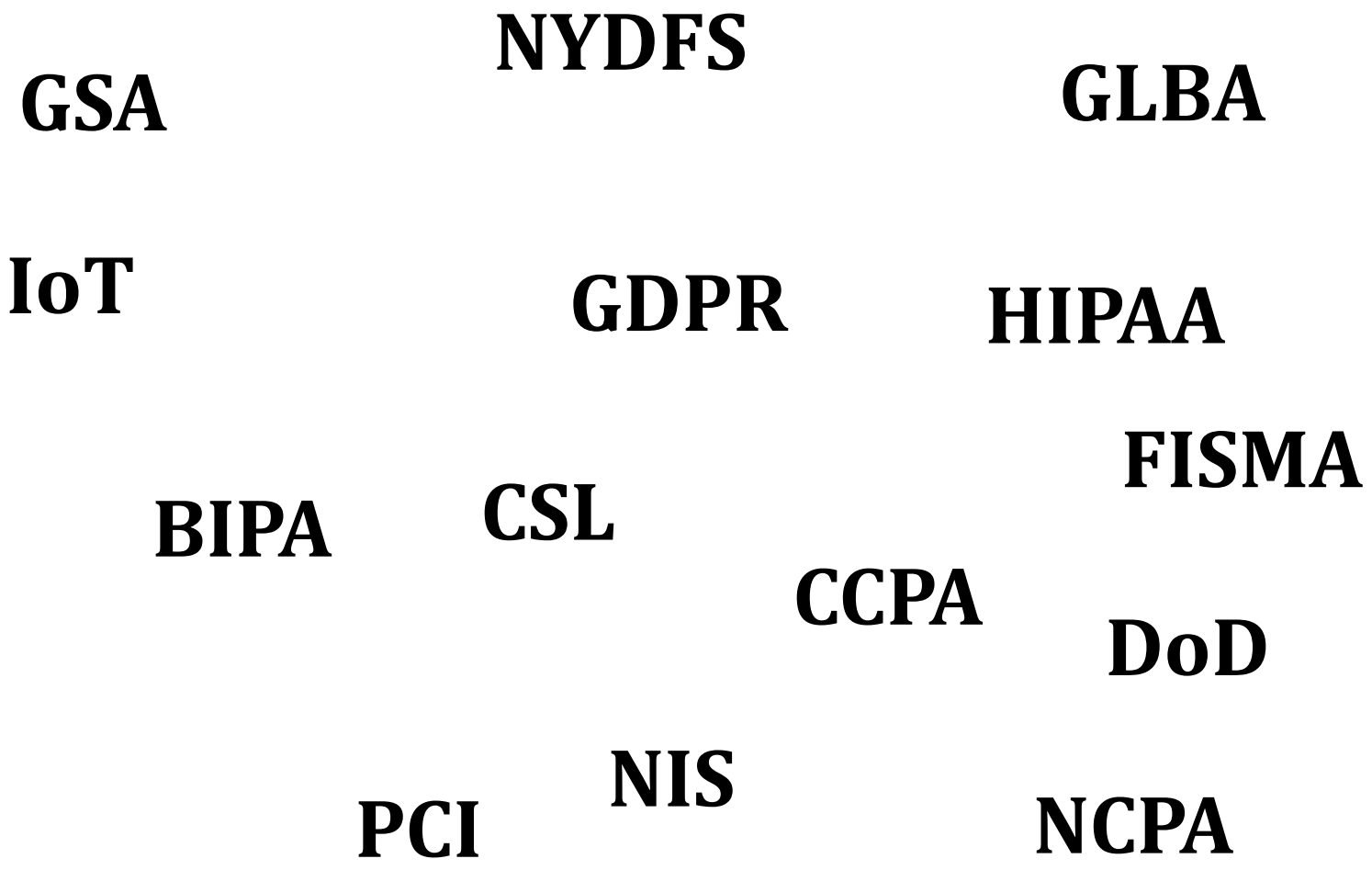
Helena Ledic
Associate General Counsel
CSC

Disclaimer: The views expressed by the presenters are not necessarily the views shared or endorsed by their corporations or CSC. This presentation is for informational purposes only and does not constitute legal advice.

Agenda

- Cybersecurity risks and importance
- External and internal threats
- Roles and responsibilities
- Preparedness and prevention
- Future directions
- Key takeaways
- Appendix

Importance of Cybersecurity – Regulations and Laws



Importance of Cybersecurity - NYDFS

Press Release

January 04, 2020

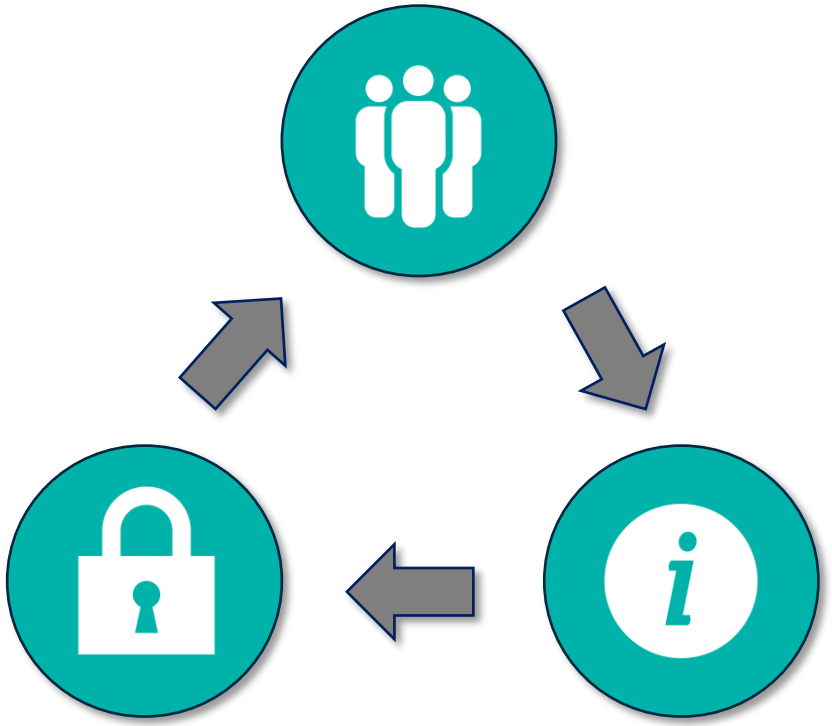
DEPARTMENT OF FINANCIAL SERVICES ISSUES ALERT TO REGULATED ENTITIES CONCERNING HEIGHTENED RISK OF CYBER ATTACKS

"DFS therefore recommends that all regulated entities ensure that all vulnerabilities are patched/remediated (especially publicly disclosed vulnerabilities), ensure that employees are adequately to deal with phishing attacks, full implement multi-factor authentication, review and update disaster recovery plans, and respond quickly to further alerts from the government or other reliable sources. It is particularly important to make sure that any alerts or incidents are responded to promptly even outside of regular business hours – Iranian hackers are known to prefer attacking over the weekends and at night precisely because they know that weekday staff may not be available to respond immediately."

https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202001041

Why Cybersecurity Is Important to You

- Your customers
- Your employees
- Your shareholders
- Your reputation
- Your paycheck (if a cyber incident brings down your company and your job)



Implications of a Security Breach

- **Average cost of a breach = $7.9 million or $233/lost or stolen record**
  - $4.2M in loss of customers/loss of good will
  - $1.8M in post-breach costs, i.e., help desk and remediation
  - $1.3M in detection and escalation
  - $600K in notification costs
- **Government authorities routinely investigate and seek monetary payments**
  - **HHS** (June 2018): $4.3M penalty imposed on cancer care center following thefts of an unencrypted laptop and of two thumb drives exposing PHI of 33,500 individuals
  - **MA AG** (November 2017): $100K settlement with billing service following the theft of an unencrypted laptop put at risk the personal information of more than 2,600 children
- **Hundreds of class action lawsuits have been filed against breached entities**

Protect Your Company

- **Identify** potential internal and external threats and business risks
- **Assess** your organization's risk exposure and level of tolerance to that risk
- **Develop** security policies, procedures and compliance controls to prevent cyberattacks
- **Manage** performance and risk oversight through centralized effort of management, board and employees
- **Prepare** incident response plans

Cyber Threats

External Threats

- Nation-states
- Criminal syndicates
- Hactivists and Gray Hats

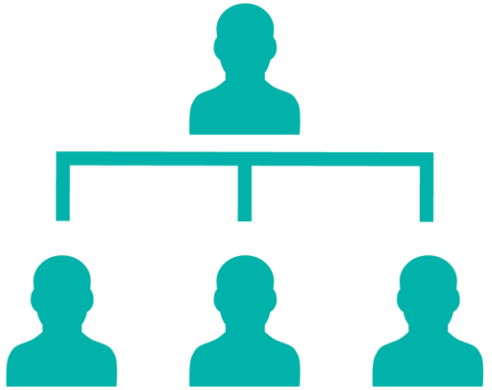
Internal Threats

- Employee actions
- Third-party vendors
- Faulty processes and procedures

Security is Everyone's Responsibility

Spread awareness of and responsibility for cybersecurity to everyone in the organization

- IT
- Physical Security
- Compliance
- Legal
- Corporate Communications
- Marketing
- HR



In-House Counsel's Role

- **Establish and encourage good governance**
  - Focus on enterprise wide risk assessment and tolerance
  - Align cyber activities and spend to strategic priorities of the organization and its risk profile
  - Monitor metrics, security plans/policies
- **Risk assess your third party vendors**
- **Support awareness and governance by the Board of Directors**
  - Duty of care and fiduciary responsibility to shareholders
  - Board meeting discussions
    - Risk identification and oversight
    - Cybersecurity strategic initiatives and planning
  - Directors need to be aware of their responsibilities surrounding cyber security
  - Limitation of liability under Del. Code Ann. tit. 8, § 102 and *Caremark* line of cases
- **Distill legal requirements to plain language for business stakeholders**
- **Support in a data incident investigation, remediation and response**

Cybersecurity Governance - Preparedness

- Preemptively hire outside counsel and consider having outside counsel hire all outside vendors including forensics and PR
- Run tabletop exercises annually (best practice – quarterly); consider having outside counsel there
- Audit the tabletop exercises to get an action plan for your next tabletop
- Document the gaps and review future results to see if the deficiencies were addressed
- Define party's roles and responsibilities, tracking, monitoring, etc.
  - Employees
  - Outside Counsel
  - Vendors
  - Insurance carrier
- Evaluate ways to reach employees and others
  - Paper
  - Personal emails/cells
  - Non-networked laptops
  - Flash drives

Cybersecurity Governance - Prevention

- Conduct customized ongoing employee cybersecurity training
- Review and communicate internal policies
- Vendor assessments-review customer and vendor agreements for security language and continue to be mindful of changing and emerging technologies
- Exercising audit rights, conducting IT Risk Assessments, Pen Tests, etc.
- Manage company's digital assets
  - Inventory – URLs, apps, vanity sites
  - Determine management responsibility
  - Consider centralizing and consolidating to secure and protect
  - Monitor social media/enforce social media use policies
- Monitor email, website traffic and brands
- Include procurement for cybersecurity evaluations

The Future State of Affairs

New York State Department of Financial Services

- 23 NYCRR 500
- Financial Institutions and Financial Services Companies
- Very limited exemptions based on revenues and number of employees
- Annual reports by CISO
- Aligns with NIST
- Vendor management policies
- Multi-Factor Authentication

Department of Defense – Cybersecurity Maturity Model Certification (CMMC)

- All companies doing business with DoD
- June 2020 target for Requests for Information
- Third-party verification
- All subcontractors
- Allowable, reimbursable cost
- Certificate duration still unknown

Sector Specific/Regional Laws

- NDAA
- GDPR
- Brazil and other countries
- "Reasonable Safeguards"

Key Takeaways

- Many cyber breaches are due to third-party vendors or insiders
- Insider threats are increasing because of nation-state actions
- Outside counsel should hire forensics and other vendors including PR
- Table tops need to be done annually (at a minimum), audited and an action plan developed for the next exercise
- Review insurance coverage (Liability, Tech E & O, Business Interruption), consolidate to same carrier
- Know your data and how it is going to be used; be proactive in addressing potential use in policies and procedures

Questions

Thank You For Attending

Brandon Pattison
Corporate Attorney
Arrow Electronics
brandon.pattison@arrow.com

Helena Ledic
Associate General Counsel
CSC
helena.ledic@cscglobal.com

Lucky Vidmar
Vice President & Senior Counsel
Head of Technology, IP, Procurement & Real Estate
Western Union
lucky.vidmar@westernunion.com

Appendix

What Is at Risk and Why This Is Important?

Companies are overlooking security risks associated with:
Domain Names, **DNS** and **Digital Certificates**

When these assets are attacked…	…applications are compromised…	…and the attack can result in:
Security risks that are proven blind spots  Domains  Digital Certificates 	**Foundational assets to run your business**  Website  Email  Corporate Applications	✓ Website redirection ✓ Email compromise ✓ Network breaches ✓ Fines (GDPR and CCPA) ✓ Brand reputation damage

Sources

- A Roadmap: How In-House Counsel Can Prepare For and Mitigate the Risk of a Cyber Attack
  https://www.acc.com/resource-library/roadmap-how-house-counsel-can-prepare-and-mitigate-risk-cyber-attack
- Top Ten Steps to Planning and Training for Security Incidents
  https://www.acc.com/resource-library/top-ten-steps-planning-and-training-security-incidents
- Cybersecurity Checklist for Boards of Directors
  https://www.acc.com/sites/default/files/resources/vl/membersonly/SampleFormPolicy/1420133_1.pdf
- NACD Corporate Governance
  https://www.nacdonline.org/insights/resource_center.cfm?ItemNumber=20789
- Department of Defense Cybersecurity Maturity Model Certification
  https://www.acq.osd.mil/cmmc/index.html
- New York Cybersecurity Requirements For Financial Services Companies
  N.Y. Comp. Codes R. & Regs. tit. 23, § 500.00
- California Data Breach Report – Standards
  - https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf

Board Responsibilities – NACD Director's Handbook on the 5 Principles of Cyber-Risk Oversight

- Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
- Directors should understand the legal and regulatory implications of cyber risks as they relate to their company's specific circumstances.
- Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the Board meeting agenda.
- Directors should set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget.
- Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

*https://www.tylercybersecurity.com/blog/cybersecurity-roles-and-responsibilities-for-the-board-of-directors

Relevant Statutes

- GDPR
- CCPA - Center for Internet Security's Top 20 Critical Security Controls (CSC 20)
  - The Basic Controls:
    - Inventory and Control of Hardware Assets
    - Inventory and Control of Software Assets
    - Continuous Vulnerability Management
    - Controlled Use of Administrative Privileges
    - Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
    - Maintenance, Monitoring and Analysis of Audit Logs
- Illinois Biometric Privacy Act (BIPA)
  - Six Flags case
  - Private cause of action
  - No injury allegation necessary

U.S. Privacy Law

- Health Insurance Portability & Accountability Act ("HIPAA"): Employee health benefits information
- Americans with Disability Act ("ADA"): Medical information received for accommodation requests, fitness-for-duty evaluations, and direct threat analysis
- Genetic Information Non-Discrimination Act ("GINA"): Genetic test results and any information concerning a disease or disorder in a family member to the 4th degree
- Fair Credit Reporting Act ("FCRA"): Regulates employment-related background checks
- Federal Wiretap Act: Generally prohibits real-time interception of communications
- Social Media Password Protection Laws: Prohibits requests for access to employees' personal online accounts