

Critical Policies for Cybersecurity Compliance

Jill Allison Opell, Esq.

Scott Lyon, Esq.



MICHELMAN & ROBINSON, LLP
ATTORNEYS AT LAW

What Types of Information do We Collect?

- **Information specific to individual**

- Social Security Number
- Account numbers
- Name
- Address
- Specific financial information

- **Catch-all**

- Information not publicly available



MIR MICHELMAN & ROBINSON, LLP
ATTORNEYS AT LAW

Now That You Have It, Protect It!

- **GLBA Safeguards Rule:** If you are going to accept responsibility for having someone's personal information, then protect it



M|R MICHELMAN & ROBINSON, LLP
ATTORNEYS AT LAW

NY DFS Cybersecurity Regulation

M|R
MICHELMAN & ROBINSON, LLP
ATTORNEYS AT LAW

New York Takes the Lead

- **3/2/16** NAIC proposes Insurance Data Security Model Law (version 2 – 8/17/16)
- **9/28/16** NY Dept. Fin. Services (NYDFS) proposes its own cybersecurity regulations for all DFS-regulated entities
- **12/28/16** NYDFS releases revised cybersecurity proposal
- **2/16/17** NYDFS regulations posted to New York State Register, to take effect on 3/1/17
- **March 2017** NAIC meeting in Denver – NYDFS proposes that other states should use its cybersecurity regulations as a model for their own legislation

NY DFS Cybersecurity Regulation

- **Effective March 1, 2017**
 - Beginning February 15, 2018
 - Required to annually prepare and submit a certification of compliance pursuant to § 500.17
 - Transition Period
 - 180 days from the effective date of the final rule to comply with requirements
- **NAIC**
 - Still working on cyber rules
 - Anticipate to look similar to NY DFS regulations



Covered Entity

- **Insurers, individual brokers, agents and adjusters have a new mandate to deal with**
 - “Maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of [their] Information Systems”
 - Designate a Chief Information Security Officer (CISO)
 - Responsible for overseeing and implementing the Covered Entity’s cybersecurity program
 - Develop written annual report which will be reviewed internally
 - May be third-party service provider but must report to management

Program Requirements

- **Must include:**

<ul style="list-style-type: none"> ✓ Penetration Testing & Vulnerability Assessments ✓ Audit Trail ✓ Access Privileges ✓ Written Procedures, Guidelines and Standards ✓ Periodic Risk Assessment ✓ Cybersecurity Personnel and Intelligence ✓ Third Party Service Provider Security Policy 	<ul style="list-style-type: none"> ✓ Multi-Factor Authentication ✓ Limitations on Data Retention ✓ Training and Monitoring ✓ Encryption of Nonpublic Information ✓ Incident Response Plan ✓ Annual Notices to Superintendent
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Deadlines

- **March 1, 2017** – effective date of regulation
 - **August 28, 2017** – 180 days
 - Implement & maintain program and policy § 500.02 & § 500.03
 - Limit **user access privileges** as part of program § 500.07
 - Utilize qualified **cybersecurity personnel** § 500.10
 - Notify Superintendent of **cybersecurity events** § 500.16
 - File **Notice of Exemption** with Superintendent
 - Designate Chief Information Security Officer [**CISO**]* § 500.04
 - Establish a written **incident response plan*** § 500.16
- * Does NOT apply to Covered Entities that qualify for the Limited Exemption § 500.19(a)

Deadlines

- **February 15, 2017**
 - Submit annual **certification of compliance** to Superintendent
 - **March 1, 2018** – one year
 - Conduct periodic **risk assessment**
 - CISO to provide **annual report to board** or governing body of agency* § 500.04(b)
 - Conduct annual **penetration testing** and bi-annual **vulnerability assessments*** § 500.05(a)(1) & § 500.05(a)(2)
 - **Multi-factor authentication** if needed* § 500.12
 - Regular **cybersecurity awareness training** for all personnel
- * Does NOT apply to Covered Entities that qualify for the Limited Exemption § 500.19(a)

Deadlines

- **September 1, 2018 – 18 months**
 - Establish policies and procedures for **data retention & disposal** § 500.13
 - Establish **audit trails*** § 500.06
 - Establish procedures, guidelines and standards for development of **in-house developed applications*** § 500.13
 - Monitor **authorized users*** § 500.14(a)(1)
 - Encryption of data both in transit over external networks and at rest* § 500.15

* Does NOT apply to Covered Entities that qualify for the Limited Exemption § 500.19(a)

Exemptions

- **Covered Entities exempt from the requirements if they**
 - Have less than the specified number of employees, gross annual revenue or year-end total assets
 - Are an employee, agent, representative or designee of a Covered Entity
 - Do not directly or indirectly operate, maintain, utilize or control any Information Systems
 - Do not directly or indirectly control, own, access, generate, receive or possess Nonpublic Information
- **Required to file a Notice of Exemption**

Cybersecurity Programs: What Do You Need?



MICHELMAN & ROBINSON, LLP
ATTORNEYS AT LAW

Who Do You Call?

- **Regulatory compliance issue**
 - Attorney client privilege/work product
- **Due diligence v. Post-breach investigation**
 - Breaches
 - Ignorance (willful or otherwise) is not an excuse
 - FTC enforcement actions - “[An unfair act or practice] causes or is likely to cause substantial injury” (15 USC 45(n))
 - 3rd Cir. in *Wyndham* case – “Wyndham was not entitled to know with ascertainable certainty the FTC’s interpretation of what cybersecurity practices are required by § 45(a). Instead, the relevant question in this appeal is whether Wyndham had fair notice that its conduct could fall within the meaning of the statute ... As a necessary consequence, Wyndham is only entitled to notice of the meaning of the statute and not to the agency’s interpretation of the statute.”

MIR MICHELMAN & ROBINSON, LLP
ATTORNEYS AT LAW

Cybersecurity Policy

- **Goal: Protection of Information Security Systems and NPI/PII, based on Risk Assessment**
 - Risk Assessment Policy (the foundation)
 - Data governance and classification (NPI/PII)
 - Incident Response Plan
 - Third Party Service Provider Security Policy
 - Asset inventory and device management (what do you have)
 - Access controls and identity management (PLP, restrictions)
 - Business Continuity and Disaster Recovery Policy
 - Customer Data Privacy policy
 - System availability plan (Ransomware, DDoS)
 - Physical security (not all administrative or technical)

Risk Assessment Policy

- **Written policies and procedures for satisfying objectives (23 NYCRR 500.09(b))**
- **Objectives:**
 - Identify assets
 - Identify threats/risks against assets
 - Prioritize threats
 - Mitigate threats



Risk Assessment Policy

- **Identify assets**
 - Company information and data
 - Hardware and software (servers and endpoints)
 - Organization's reputation and branding
 - Personnel
- **Identify threats/risks against assets**
 - System hacked from inside
 - System hacked from outside
 - Data Unavailable
 - Ransomware
 - Hardware failure
- **Analyze impact**



Risk Assessment Policy

- **Prioritize threats**
 - Ransomware – healthcare and other service providers
 - Data exfiltration – confidential information (Ashley Madison)
- **Mitigation techniques**
 - Ransomware → robust backup strategy
 - DDoS → clustered servers, load balancers
 - Insider threat → Access Control Lists, Principle of Least Privilege, DLP solutions
 - Outside threat → Firewalls, IDS, IPS, encryption
- **Residual Risk** – insurance = transferring risk

Data Governance and Classification Policy

- **Types of private/sensitive/confidential information**

- Financial
- Healthcare
- NPI/PII

- **Groups/Classes**

- Role-based, not individual
 - HR, Accounting
- Sensitivity
 - Top Secret → Unclassified

- **Principle of Least Privilege**



Incident Response Plan

- **Develop policies and procedures for responding to potential breaches** (23 NYCRR 500.16)

- “Incident” v. “Breach” v. “Cybersecurity Event”
- Internal processes for responding (ex: flow-chart)
- Roles, responsibilities and levels of decision-making authority
 - Coordinating communications - Law Enforc, Forensics, HR, PR
- External and internal communications and information sharing
- Plan for remediation of identified weaknesses
- Documentation and reporting (forensics, chain of custody)
- Evaluation and revision (Lessons Learned)

Third Party Service Provider Security Policy

- **Develop policies and procedures for Third Party Service Providers (TPSP)** (23 NYCRR 500.11)
 - Based on the Risk Assessment
 - Risk assessment of TPSP
 - Minimum cybersecurity standards (ISO, addendum)
 - Access controls
 - Encryption
 - Notification requirements
 - Due diligence processes (auditing)
 - Periodic assessment based on risk and adequacy



Disaster Recovery Plan

- **Based on Risk Assessment (fire, flood, earthquake)**
- **Business Impact Assessment (BIA)**
 - Identify critical systems
 - Prioritize recovery time objective
- **Identify preventative controls**
 - Ex: backup data centers
- **Develop recovery strategies**
 - Ex: emergency office sharing
- **Develop IT contingency plan**
 - Ex: remote login
- **Backup strategy – 3/2/1 (copies, media, offsite)**



Training and Testing Program

- **Training – educate employees**
 - Communicate business risks and consequences
- **Tabletop Simulations – executive fire drills**
 - Helps identify SPOF
 - Policy revisions
- **Penetration Testing – periodic checkup**



M|R MICHELMAN & ROBINSON, LLP
ATTORNEYS AT LAW

Consequences of Breach

- **Damages**
 - Costs of breach
 - Notification costs
 - Monitoring costs
 - Legal costs
 - FTC fines and penalties (state and federal)
 - Insurance: loss of license
- **Privilege:** Make sure your preparation and response does not turn into the evidence against you



Have a plan!

M|R MICHELMAN & ROBINSON, LLP
ATTORNEYS AT LAW



Questions?

MIR
MICHELMAN & ROBINSON, LLP
ATTORNEYS AT LAW



Thank You!



Jill Allison Opell, Esq.
jaopell@mrlip.com

Scott Lyon, Esq.
slyon@mrlip.com

MIR
MICHELMAN & ROBINSON, LLP
ATTORNEYS AT LAW