# NY DFS Cybersecurity Cybersplained

## Triangle InfoSecCon 2018

Manny Landron, CISO, IAT Insurance Group

IAT Insurance Group

# Agenda

- Cybersecurity Regulations
- Cybersecurity Program
- Risk Assessment
- Cybersecurity Policy
- Access Management
- Cybersecurity Personnel
- Incident Response Plan
- Chief Information Security Officer
- Notices to NY DFS Superintendent

# Agenda

- Penetration Testing and Vulnerability Assessment
- Multifactor Authentication (MFA)
- Encryption of Non Public Information (NPI)
- Security Awareness Training
- Security Monitoring
- Audit Trails
- Secure Disposal of Non Public Information (NPI)
- Application Security
- Third Party Risk Management
- Impact of South Carolina Act

# Cybersecurity Regulations

- 23 NYCRR 500 – Cybersecurity Requirements for Financial Services Companies
- National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law
- South Carolina Insurance Data Security Act

# Cybersecurity Program

- Maintain a **risk-based** cybersecurity program **based on a risk assessment** that focuses on protecting **nonpublic personal information.**

# Risk Assessment

- Conduct a **periodic** risk assessment and update as reasonably necessary to address changes to the environment.

**Note:** South Carolina requires an annual risk assessment.

# Cybersecurity Policy

- Implement and maintain a **written** cybersecurity policy **approved by the Board of Directors (BoD).**

# Access Management

- Limit user access privileges to information systems and **periodically review such access** privileges.
  - Identity and Access Management – **Manual vs Automated**
  - Privileged Access Management
    - Network and Server Infrastructure
    - Workstations
    - Active Directory
    - Applications
- File Activity Monitoring – Folder and File Access

# Cybersecurity Personnel

- Employ **qualified** cybersecurity personnel to manage cybersecurity risk and provide personnel with training sufficient to address cybersecurity risk.
- Verify that personnel maintain current knowledge of changing threats and countermeasures.

# Incident Response Plan

- Establish a **written** incident response plan designed to promptly respond to and recover from any cybersecurity incident materially affecting the confidentiality, integrity or availability of information systems or business operation.

# Chief Information Security Officer (CISO)

- Designate a CISO or a **qualified** individual responsible for overseeing and implementing the cybersecurity program.
- CISO shall **report in writing** the state of the cybersecurity program and **material** cybersecurity risks and events, at least annually, to the Board of Directors (BoD).
- What is material????

# Notices to NY DFS Superintendent

- Notify the superintendent as promptly as possible but no later than **72 hours** from a determination that a cybersecurity incident occurred if the event
  - Is reportable to a government, self-regulatory, or supervisory body.
  - Has a reasonable likelihood of **materially** harming any part of normal operation(s).
- Annually, **on February 15**, submit to the superintendent a written statement **signed by the Chairperson of the Board of Directors** covering the prior calendar year certifying that the company complies with requirements and **maintain supporting evidence for 5 years.**

# Penetration Testing and Vulnerability Assessments

- Conduct an **annual** penetration test and biannual vulnerability assessments.

**Note:** These are minimum requirements.

# Multifactor Authentication

- Multifactor Authentication (MFA) shall be utilized for any individual accessing the internal network from an external network.
- Enable MFA:
  - On you Virtual Private Network (VPN).
  - On critical Software-as-a-Service (SaaS) application such as email, content collaboration, i.e. O365, Box, etc…
  - For Infrastructure-as-a-Service (IaaS) admins.
  - To your privileged access management solution.

# Encryption of Non Public Information

- Implement controls, including encryption, to protect nonpublic information in transit or at rest (if feasible).
  - Email
  - File transfer
  - Removable media
  - Offsite backups

# Security Awareness Training



- Provide **regular** cybersecurity awareness training for all personnel.
  - Annual end user security awareness training.
  - Monthly Newsletters (SANS Ouch!).
  - Train your developers and administrators.
  - Be careful with phishing and social engineering tests.

# Security Monitoring

- Monitor the activity of authorized users and **detect unauthorized access**, use of or tampering with nonpublic information by authorized users.
  - Network Security Monitoring
  - Endpoint Security monitoring
  - File Activity Monitoring
  - Intrusion Detection (Prevention)
  - DNS ad URL Filtering
  - File Activity Monitoring

# Audit Trails



- Maintain audit trails necessary to reconstruct
  - Financial **transactions** for **5 years**
  - Cybersecurity **events** for **3 years**

- **Note:** Events can be defined broadly to include those that are successful and unsuccessful. NY DFS anticipates that most unsuccessful attacks will not be reportable, but seeks the reporting of those unsuccessful attacks that, in the considered judgment of the Covered Entity, are sufficiently serious to raise a concern.

# Secure Disposal of Non Public Information

- Maintain and implement a policy to securely dispose of nonpublic information no longer necessary for business operations or for other legitimate business purposes **except** where such information is required to be retained by law or regulation.
  - Paper
  - Electronic Media
  - Data Retention Schedule

# Application Security

- Maintain **written** procedures, guidelines and standards to ensure secure development practices for **in-house developed apps** and procedures for evaluating the security of **external apps** used by the company.
  - Secure Coding Standards
  - Code Reviews
  - Developer Security Awareness Training
  - Web Application Vulnerability Assessments
  - Web Application Pen Test
  - Static and Dynamic Code Analysis

# Third Party Risk Management

- Identify and **periodically** risk assess **third party service providers** including their use of multifactor authentication, encryption, cybersecurity incident reporting and **representation of warranties**.
  - Manual vs Automated?
  - SIG or not?
  - Inventory and risk rank 3rd party service providers (cost driver).
  - Security Addendum

**Note:** Due March 1, 2019

# Impact of South Carolina Act

- South Carolina Insurance Data Security Act **based on NAIC Model Cybersecurity Law** and compliance **due by July 1, 2019.**
- Incremental difference between NY DFS cybersecurity requirements and SC act:
  - Manage cybersecurity risk as part of enterprise risk management (ERM) process.
  - Perform annual cybersecurity risk assessment and program audit.
  - Notify consumers in the event of a data breach **if greater than 250 consumers impacted.**
  - Author and communicate (consumer) privacy policy because you have to provide it in the event of a reportable event.

# Thank You!

## Questions? | Discussion

IAT Insurance Group