Monday, April 15 11:15 AM - 12:45 PM
OM10: Cybersecurity Track (Session 1):
Cyber Scenario: Simulated Firm Attacks

AGENDA

- Introductions
- Common Cyber Threats and Trends
- Overview of Data Privacy and Cybersecurity Laws
- Key Issues in Privacy and Cybersecurity for Law Firms
- Basic Cyber Incident Response Planning
  - Internal Policies
  - External Issues
  - Operations and Technical Issues
  - NIST, SANS and ISO Standards and Technical Processes and Practices
  - Training
  - Security Incident Response Team Members
  - Other?
- Table Top Scenrio
How can we secure something if we don’t know what it is?

- In 2017, cyber attacks cost small and medium-sized businesses an average of $2,235,000.  
Ponemon 2017 State of Cybersecurity in SMBs

- 92.4% of malware is delivered via email.  
Verizon 2018 DBIR

- 60% of small businesses say attacks are becoming more severe and more sophisticated.  
Ponemon 2017 State of Cybersecurity in SMBs

Disaster Redefined:  
A data breach is now considered more damaging than fire, flood, theft and transit strike

Think you know what could cripple a small or medium business in America? Think again. More Small-to-Medium-sized Businesses (SMBs) executives now believe a data breach is more detrimental and more likely to end their business than traditional disasters.
Here are some other numbers that reflect the scale of the ransomware problem:

- Ransomware attacks rose 350% worldwide from 2016 to 2017 (Dimension Data, 2018)
- An increase in ransomware-related support inquiries in the past year was noted by 48% of IT consultants across 22 different industries (Intermedia, 2017)
- 25% of cyber insurance claims in 2017 were ransomware (AIG, 2018)
- Total losses due to WannaCry ransomware could reach $4 billion (Cyence, 2017)
- 72% of businesses hit by ransomware lost access to data for at least two days; 32% lost access for five days or more (Intermedia, 2017)

Source: Symantec 2018 Internet Security Threat Report (ISTR)
COMMON MISPERCEPTIONS ABOUT RANSOMWARE ATTACKS

<table>
<thead>
<tr>
<th>Misperception</th>
<th>Truth</th>
</tr>
</thead>
</table>
| “Everyone gets hit by ransomware. It’s no big deal as long as you get the hackers to unlock the data.” | ▪ Most large breaches are the product of smaller, unresolved incidents.  
 ▪ Significant breaches almost never appear to be significant on day one.                                                                                                                    |
| “Our technical teams decrypted the data, so case closed.”                    | ▪ Ransomware can act as an anti-forensic tool rather than an end unto itself, which means that it’s designed to fool you.  
 ▪ Hackers frequently leave behind malware that allows them to remain in your system.  
 ▪ Depending on the jurisdiction(s) you operate in, the fact that some types of data were accessed by the ransomware may trigger regulatory inquiries or statutory requirements. |
| “This only impacted a handful of machines.”                                   | ▪ Depending on how the ransomware was deployed, it may be a symptom of a larger compromise.                                                                                                               |

COMMON CYBER THREATS AND TRENDS

Mobile malware continues to surge

- Threats in the mobile space continue to grow year-over-year. The number of new mobile malware variants increased by 54 percent in 2017, as compared to 2016.

- And last year, an average of 24,000 malicious mobile applications were blocked each day.

Source: Symantec 2018 Internet Security Threat Report (ISTR)
COMMON CYBER THREATS AND TRENDS

Coin mining attacks explode

- Cyber criminals who have been firmly focused on ransomware for revenue generation are now starting to explore other opportunities.
- During the past year, the astronomical rise in cryptocurrency values inspired many cyber criminals to shift to coin mining as an alternative revenue source.
- This coin mining gold rush resulted in an 8,500 percent increase in detections of coinminers on endpoint computers in 2017.

Source: Symantec 2018 Internet Security Threat Report (ISTR)

BRIEF OVERVIEW ON DATA PRIVACY AND CYBER LAWS

- US cybersecurity and data privacy laws are, to put it lightly, a mess.
- Years of piecemeal legislation, Supreme Court decisions, and government surveillance crises, along with repeated corporate failures to protect user data, have created a legal landscape that is, for the American public and American businesses, confusing, complicated, and downright annoying.
- As of April 2018, every single US state has its own data breach notification law.
KEY ISSUES IN PRIVACY AND CYBER SECURITY FOR LAW FIRMS

- Legal Ethics
- ABA Formal Opinion 477R—Securing Communication of Protected Client Information
- ABA Formal Opinion 483—October 17, 2018—Lawyers’ Obligations After an Electronic Data Breach or Cyberattack
- Model Rules 1.1, 1.6, 5.1 and 5.3

THE UNIVERSAL PROBLEM
BASIC CYBER INCIDENT RESPONSE PLANNING

- Internal Policies
- External Issues
- Operations and Technical Issues

INTERNAL POLICIES

Passwords
- Establish a standard for creating strong passwords and frequency of change
- Privilege Management – Authorized User Rights will be granted using the least-privilege methodology, based on business need and security requirements.

User Password Management
- User’s account and password are the primary means of verifying a user’s identity and allocation of passwords is a formal management process.
- Review of User Access Rights – Review of all Privileged and Authorized Users right to ensure they are consistent with their present job function.

Back-up – Retention/Destruction policies
- Information must not be retained any longer than the business/applicable regulation requires it to be retained
- Must be kept no longer than needed for operation
- Who is responsible for updating backups? – company or user
INTERNAL POLICIES

Unattended User Equipment
- Users must protect the firm’s information resources from unauthorized access by protecting unattended computer equipment.

User Identification and Authentication
- Users will be identified and authenticated with the minimum of a unique identification and password before access to firm workstations is granted.

User Account Review/Audit
- Users are reviewed on a regular basis to ensure malicious, out-of-date or unknown accounts do not exist.

INTERNAL POLICIES

Mobile Computing
- Ensuring that business information is not compromised by use of devices such as notebooks, laptops, tablets and mobile phones in an unprotected environment and provide users with controls for and awareness of risks.

Wireless Connections/Remote Access
- Ensure the control and protection of firm’s informational resources against possible threats.

Cloud Storage/Removable Media
- May use only approved, password-protected removable media in their work computers with permission.
INTERNAL POLICIES

Security Awareness Training
• Content reviewed and disseminated by CISO and updated as appropriate and a minimum level of training for all users including updates of:
  • Updates of policies for protecting IT systems and data
  • Separation of duties and privilege
  • Prevention and detection of information security incidents
  • Proper disposal of data storage media
  • Proper use of encryption

Social Media Policies
• Allowing users to associate themselves with the company when posting but must clearly brand their online posts as personal and purely their own

BYOD
Bring Your Own Device policies
Who is in charge of the content on the device?
Are there regulations about what can be sent from and to that device?
What happens if that device is lost?

INTERNAL ISSUES

Data Classification
• **Client Information** – including all information collected during the onboarding process
• **Privileged information** – all information that is protected by attorney-client privilege
• **Human Resources Information** – including payroll info, employee reviews, incident reports, harassment claims, benefit’s information, credit reports, background checks
• **HIPAA information** – an individual’s medical, health-related or health insurance-related information
• **Company information** – including trade secrets, methodologies, business strategies, business plans, information about clients, competitor-sensitive information
• **Personal Identifying Information (PII)** – information that can be used on its own or with other information to identify, contact or locate an individual
EXTERNAL POLICIES

- Privacy Policies –
  - Start with a questionnaire
- Contracts/Third-party access
  - Who is authorized?
- Security Requirements

FRAMEWORKS

- Compliance
  - Requirements
  - Regulations
  - Policies
  - Standards
  - Transparency
  - Law
  - Rules
The National Institute of Standards and Technology (NIST) created and released the “Framework for Improving Critical Infrastructure Cybersecurity” on February 12, 2014. This Framework, also referred to as the NIST Cybersecurity Framework (CSF), created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on organizations.

- The NIST CSF provides a uniform guide for developing robust cybersecurity programs for organizations. This includes industry-driven standards, best practices and implementation measures to manage cybersecurity risks to information technology and operational technology. NIST CSF is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles.
- Each Framework component reinforces the connection between business drivers and cybersecurity activities.
SANS Institute along with the Center for Internet Security (CIS) created a security framework – Critical Security Controls (CSC) for Effective Cyber Defense.

- Provides specific and actionable ways to stop today’s most pervasive and dangerous attacks by prioritizing and focusing on a smaller number of actions with high pay-off results
- SANS supports the CIS CSC with training, research and what works
ISO STANDARDS

- ISO/IEC 27000 family of standards helps organizations keep information assets secure.
- Using the family of standards helps organizations manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.

SOC FOR CYBERSECURITY

SOC - SERVICE ORGANIZATION CONTROLS

SOC - SYSTEM AND ORGANIZATION CONTROLS

SOC FOR SERVICE ORGANIZATIONS
- SOC 1® - ICFR
- SOC 2® - TRUST SERVICES CRITERIA
  - SOC 2® HITRUST
  - SOC 2® CSA STAR
  - Attestation
- SOC 3® - GENERAL USE REPORT

SOC FOR CYBERSECURITY

SOC FOR VENDOR SUPPLY CHAINS
UNDER DEVELOPMENT
WHO’S INTERESTED IN YOUR CYBER PRACTICES?

Information regarding the effectiveness of an Entity’s Cybersecurity practice is needed by:

- Those charged with governance – Board of Directors
- Investors
- Lenders
- Customers
- Regulators
- Vendors & Business Partners

TRAINING

- Create a team of Security Incident Response Team Members
- This team creates, disseminates and understands the policies and procedures around security incidents pertaining to reporting, actual breach action and notification procedures, disciplinary action, and more.
TABLE TOP SCENARIOS

- Lost or Stolen Laptop
- Phishing Attack – Credential Harvesting
- Wire Transfer Fraud
- Ransomware
- BYOD – Bring Your Own Disaster Device
CYBER BREACH USE CASE DISCUSSION

- Who in our audience knows if their firm / company has a written response plan?
- If a plan exists do you know if any table-top exercises “practice runs” were conducted?
- Have you considered going beyond practice runs to really test real life attack?
- Is there a difference between a breach versus unauthorized access?
- Would you label as inappropriate use of data employees downloading case data?
- Would you react differently if you encountered Ransomware versus a Phishing Attack?
- Do you thoroughly test and evaluate your third party providers regularly?

KEY TAKEAWAYS

- It is not a question of if but when
- Know and test for your weaknesses
- Know where is your data and who has access
- Invest now with breach cost reduction tips
- Thoroughly test your third party network regularly
- Embrace the cloud – don’t be overly skeptical
THANK YOU / QUESTIONS ??

Rob Kleeger
Founder and Managing Director
Digital Forensic Investigations | Incident Response Data Breaches | Cyber Security
rkleeger@Digital4nxGroup.com
973.699.0167

Joe Riccie
Partner
Cyber & Information Security Services
jriccie@withum.com
908.303.2354