CYBERSECURITY THREATS: WHEN WILL IT HAPPEN TO YOU

Iris Ikeda

Commissioner of Financial Institutions

Department of Commerce and Consumer Affairs

May 2018

TOPICS

What is a cyber threat?

Cyber Hygiene

What to do if you are the target

WHAT IS A CYBER THREAT?

- Your day starts at 5:30 am. You check your social media sites and wish friends happy birthday. You check to see what events are going on this evening or this weekend.
- Time to exercise. You grab your Fitbit, hit the treadmill and exercise.
- During breakfast you grab your iPad or tablet and catch up on the daily news, check weather and traffic while listening to Alexa or Hey Google.
- You log into your Pop Money account and pay a friend back for yesterday's lunch.
- Your schedule Lyft to take you and your friends out this evening.

WHAT IS A CYBER THREAT?

- Time for work. You grab your phone and head out the door. You turn on the Bluetooth so you can get updates on traffic and calls via your car stereo.
- You step into your office door and cannot remember if you locked the door and set the alarm. You activate the lock and alarm with your phone and turn off the air conditioner.
- During the day you check your bank and investment accounts, use your phone to deposit a check. OnStar lets you know your car needs an oil change.
- End of work day. You order pizza to be delivered on your mobile app, turn on the air conditioning.
- You pick up milk and eggs with Apple Pay or Google wallet after you check the refrigerator app to see that you are running low.

WHAT IS A CYBER THREAT?

- At home, you log into your Pelaton class via your smart TV then Skype your friends to have dinner together.
- Before you go to bed you pay a couple of bills via your laptop, deposit a check with your phone, buy new shoes, transfer money to your college son, and finally make sure your Fitbit is auto-synced, answer emails and update your social media.

WHAT IS A CYBER THREAT?

- How much information about you did you transmit today?
- Do you use Alexa or Hey Google at work?
- How is that information being protected? By whom?
- Where is the information stored?
- How is the information being used?
- When and how is the data destroyed?

WHAT IS A CYBER THREAT?

- Information security deals with all data and information in all formats.
  - Hard copies
  - Electronic
  - Intellectual property
- Cybersecurity is a subset of information security.
  - It implements key data management controls.
  - It protects any device that connects to the web, programs, apps & data from unauthorized access.

WHAT IS A CYBER THREAT?

- Information privacy is the right to have some control over how your personal information is collected and used.
- Data privacy is how our personal data is used. Privacy departments focus on developing policies to ensure personal information collected, shared, and used in appropriate ways.
- Cyber security is about protecting electronic information & data from vulnerabilities.
- Cyber threat is anything that threatens the protected information & data.

WHAT ARE THE ETHICS OF A CYBER THREAT?

Duties of Attorneys

- Protect client information and may have contractual and regulatory duties.
- Competence (ABA Model Rule 1.1) requires attorneys to know what technology is necessary and how to use it.
  - This "requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."
  - It includes competence in selecting and using technology.
- Confidentiality (ABA Model Rule 1.6) is one of an attorney's most important ethical responsibilities.
  - Requires protection of "information relating to the representation of a client".
  - It is not limited to confidential communications and privileged information.

WHAT ARE THE ETHICS OF A CYBER THREAT?

Duties of Attorneys (con't)

- Responsibilities of a Partner or Supervisory Lawyer and Responsibilities Regarding Nonlawyer Assistant require that those under their supervision comply with these requirements.
- Model Rule 1.4, Communications, also applies to attorneys' use of technology.
  - It requires appropriate communications with clients "about the means by which the client's objectives are to be accomplished".
  - It requires keeping the client informed and, depending on the circumstances, may require obtaining "informed consent."
  - It requires notice to a client of compromise of confidential information relating to the client.

WHAT ARE THE ETHICS OF A CYBER THREAT?

- May 2017, the American Bar Association's Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477 which covered a range of issues for attorneys to consider in order to protect confidential client information from "nefarious actors throughout the internet."
- 3 ethical duties: competence, communication and confidentiality.
- The opinion recognized that the internet – "and our 24/7 reliance on smartphones, mobile devices and online technology – has changed how these principles apply to the daily work of a practicing attorney."

WHAT ARE THE ETHICS OF A CYBER THREAT?

Formal Opinion 477 (con't)

- In 2012, the ABA revised Model Rule 1.1 (Competence) to require lawyers to "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."
- The ABA tweaked Model Rule 1.6 (Confidentiality) by adding new language: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."
- In most circumstances, says the ABA, a lawyer may transmit client information over the internet if "reasonable efforts" are made to prevent inadvertent or unauthorized access. But "special security precautions" may be called for when:
  - Required by an agreement with the client.
  - Required by law.
  - Required by the "nature of the information."

WHAT ARE THE ETHICS OF A CYBER THREAT?

Seven Key Considerations – Formal Opinion 477

- **The nature of the threat.** Some client info, especially proprietary info may present a higher risk of data theft.
- **How client confidential info is stored and sent**. Every access point could be a vulnerability."
- **The use of reasonable electronic security measures**. Use Malware/AntiSpyware/Antivirus software on all devices where client info is stored
- **How electronic communications should be protected**. Some client info require different levels of protection.
- **The need to label client information as privileged and confidential.** Disclaimers in emails.
- **The need to train lawyers and nonlawyer assistants**. Establish policies & procedures and training.
- **The need to conduct due diligence on vendors who provide technology services**. Guidance in this regard can be found in ABA Formal Opinion 08-451.

WHAT IS A CYBER THREAT?

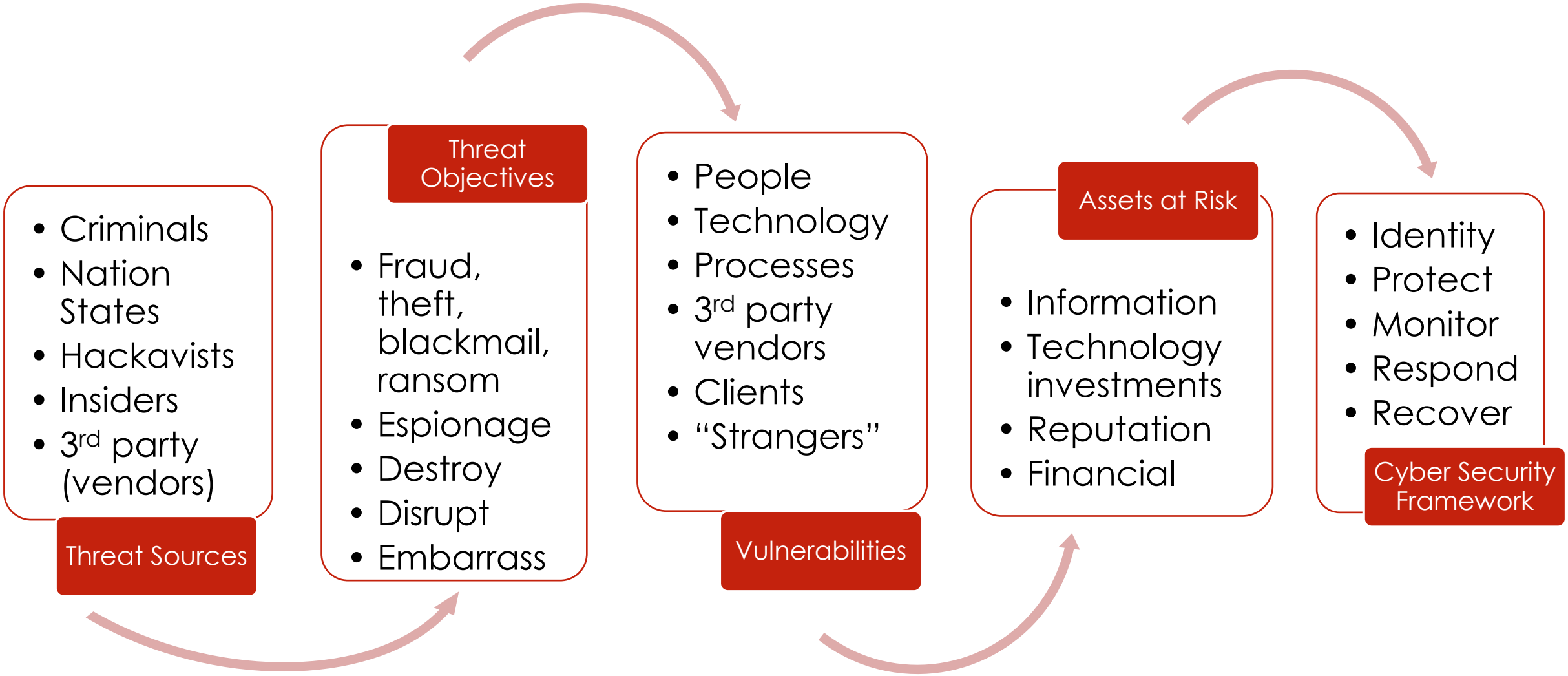
- During the day – how many times was personal information shared and potentially endangered?

- That's why we are talking about Cyber Threats and Cyber Hygiene

CYBER HYGIENE

- IDENTIFY internal and external cyber risks
- PROTECT organizational systems, assets, and data
- DETECT system intrusions, data breaches, and unauthorized access
- RESPOND to a potential cybersecurity event
- RECOVER from a cybersecurity event by restoring normal operations & services

CYBER HYGIENE FRAMEWORK

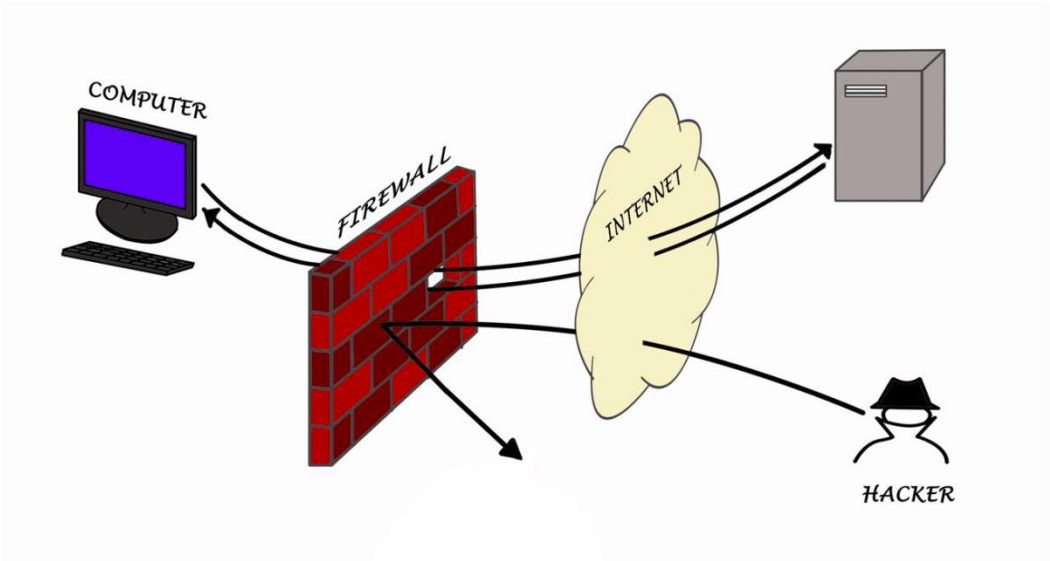


CYBER: IDENTIFY

- Risk assessment
  - Classify your “crown jewels”
  - Identify threats & vulnerabilities
  - Measure risk
  - Communicate risk

CYBER: PROTECT

- Cyber hygiene:
  - Steps computer users take to protect and maintain systems & devices.
- Customer authentication
- Access controls
- Data security



Source: CSBS

CYBER: DETECT

DETECT tools are the reinforcement of the Protect tools

- Intrusion Detection Systems;
- Network Behavior Anomaly Detection Tools;
- Security Information and Event Management /Log Analyzer;
- Configuration Management Tools; and
- Integrity Monitoring Tools.

CYBER: DETECT EXAMPLES

Common cyber-attacks that CEOs should particularly know about and understand are:

- Distributed Denial of Service (DDoS) attacks;
- Corporate Account Take Over (CATO) attacks; and
- CryptoLocker attacks.

CYBER: RESPOND

Cybersecurity data breaches are now part of our way of life.

- The Incident Response Plan
- Communicating the Data Breach
  - State law on notification
- You've Been Hacked/Attacked, What Are Your Next Steps?
- The following are three steps to consider:
  - Triage/Evaluate the Cyber-event;
  - Invoke the Incident Response Plan; and
  - Review the effectiveness of the plan.

CYBER: RECOVER

Restore & Review

- Recover infrastructure – step-by-step plan to rebuild
- Restore data – use back up data
- Reconnect service – this may take weeks to restore normal operations

ATTACK LIFECYCLE

Methods of Attack

- Email/link/embedded malware
- Vulnerable website
- Direct access to physical or wireless network
- Exploit weakness in personally owned equipment
- Exploit client or service provider weakness
- Insider abuse

CYBER HYGIENE

Planning

- Who has the lead responsibility for different elements of the cyber incident
- How to contact critical personnel 24/7
- How to proceed if critical personnel is unreachable
- Protect the crown jewels
- How to preserve data related to the intrusion
- How to determine whether data owners, clients or partner companies need to be notified
- Procedures for notifying law enforcement

CYBER HYGIENE

Back up

- Have ready access to technology & services
- Off-site data back-up
- Intrusion detection capabilities
- Data loss prevention technologies
- Devices for traffic filtering or scrubbing
- Servers should be configured to ID a network security incident
- Install software updates

CYBER HYGIENE

Network monitoring

- Real-time monitoring
- Computer user agreements, workplace policies & training

CYBER HYGIENE

Cyber Incident management

- Cyber incidents can raise unique legal questions
- Have ready access to advice from layers familiar with cyber incident response

CYBER HYGIENE

Up-to-date policies

- Review personnel and human resource policies
- IT policies
- Reasonable access controls on networks

WHAT TO DO IF YOU ARE THE TARGET STEP 1: INITIAL ASSESSMENT

- Immediately make an assessment of the nature and scope of the incident
- Have appropriate network logging capabilities
- Identify: users, connections, processes, open ports
- External communications
- Look for evidence of criminal incident

WHAT TO DO IF YOU ARE THE TARGET STEP 2: MINIMIZE DAMAGE

- Reroute network traffic
- Filter or block a distributed denial-of-service attack or
- Isolate all or parts of the compromised network
- Block illegal access
- Keep detailed records of steps taken to mitigate the damage and any associated costs
- Abandon network & restore with back-up file

WHAT TO DO IF YOU ARE THE TARGET
STEP 3: RECORD & COLLECT INFORMATION

- Create a “forensic image” of the affected computers
- Locate back ups
- Use new or sanitized equipment
- Restrict access to protect data

WHAT TO DO IF YOU ARE THE TARGET STEP 3: RECORD & COLLECT INFORMATION

- Describe all incident-related events, including dates and times;
- Include incident-related phone calls, emails, and other contacts;
- Identify persons working on tasks related to the intrusion;
- Identify the systems, accounts, services, data, and networks affected and describe how these network components were affected;
- Retain information relating to the amount and type of damage inflicted by the incident, important in civil actions and criminal cases;
- Know the type and version of software being run on the network; and
- Are there peculiarities in the firm's network architecture, like proprietary hardware or software.

WHAT TO DO IF YOU ARE THE TARGET
STEP 4: NOTIFY

- People in your firm
- Law enforcement
- Other potential victims

WHAT NOT TO DO AFTER A CYBER INCIDENT

- Do NOT used the compromised system to communicate
- Do NOT hack into or damage another network

RECOVERY

- Continue to monitor the network for any unusual activity
- Continue to monitor the network to make sure the intruder is expelled
- Conduct a post-incident review to identify deficiencies in planning and execution

CONTACT

Iris Ikeda, Commissioner
Division of Financial Institutions
Department of Commerce & Consumer Affairs
808.586.2820
Email: dfi@dcca.Hawaii.gov
Twitter: @HawaiiDFI