Cyber Security - Basics

Iris Ikeda, Commissioner

Division of Financial Institutions

Department of Commerce and Consumer Affairs

July 2016

2015 Cyber Security Incidents

- Hackers breached the systems of health insurer Anthem, Inc., exposing nearly 80 million personal records.
- Ashley Madison, the adultery website that promised its members discrete affairs
- An unknown group infiltrated hundreds of banks in multiple countries, swiping somewhere in the neighborhood of $1 billion.
- About 15 million T-Mobile customers had their information stolen after the credit-checking company Experian was breached.
- A breach of children's toy manufacturer VTech resulted in the release of records on 4.8 million parents and more than 6.8 million kids.
- The US government agency in charge of background checks was breached, exposing information on virtually every federal employee since the year 2000.

DCCA
HAWAII
Division of Financial Institutions

Agenda

- What is a cyber threat?
- Cyber Hygiene
- What to do if you are the target

Cyber Security

- 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

DCCA
HAWAII
Division of Financial Institutions

Framework

- Criminals
- Nation States
- Hackavists
- Insiders
- Third parties (vendors)

Threat Sources

Threat Objectives

- Fraud, theft, blackmail, ransom
- Espionage
- Destroy
- Disrupt
- Embarrass

- People
- Technology
- Processes
- 3rd party service providers
- Clients
- 3rd parties with no relationship with you

Vulnerabilities

Assets at Risk

- Information
- Technology investments
- Reputation
- Financial

- Identity
- Protect
- Monitor
- Respond
- Recover

Cyber Security Framework

DCCA HAWAII Division of Financial Institutions

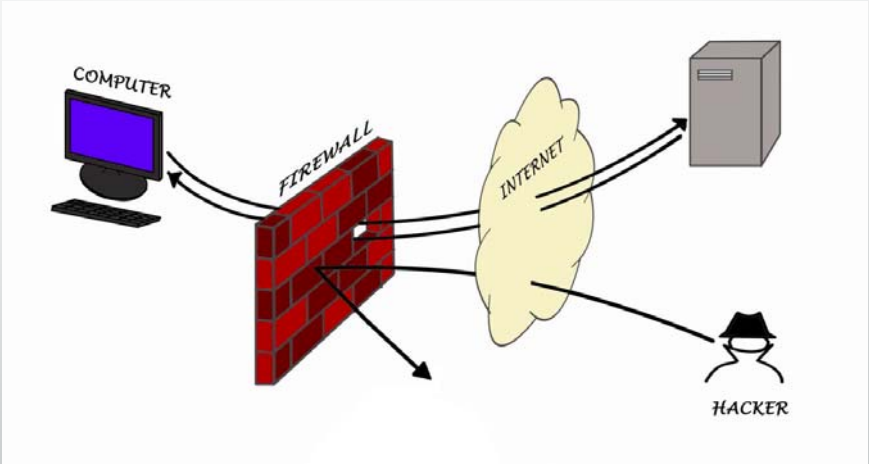
Cyber: IDENTIFY

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

DCCA HAWAII Division of Financial Institutions

Cyber: PROTECT

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



Source: CSBS

DCCA HAWAII Division of Financial Institutions

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.

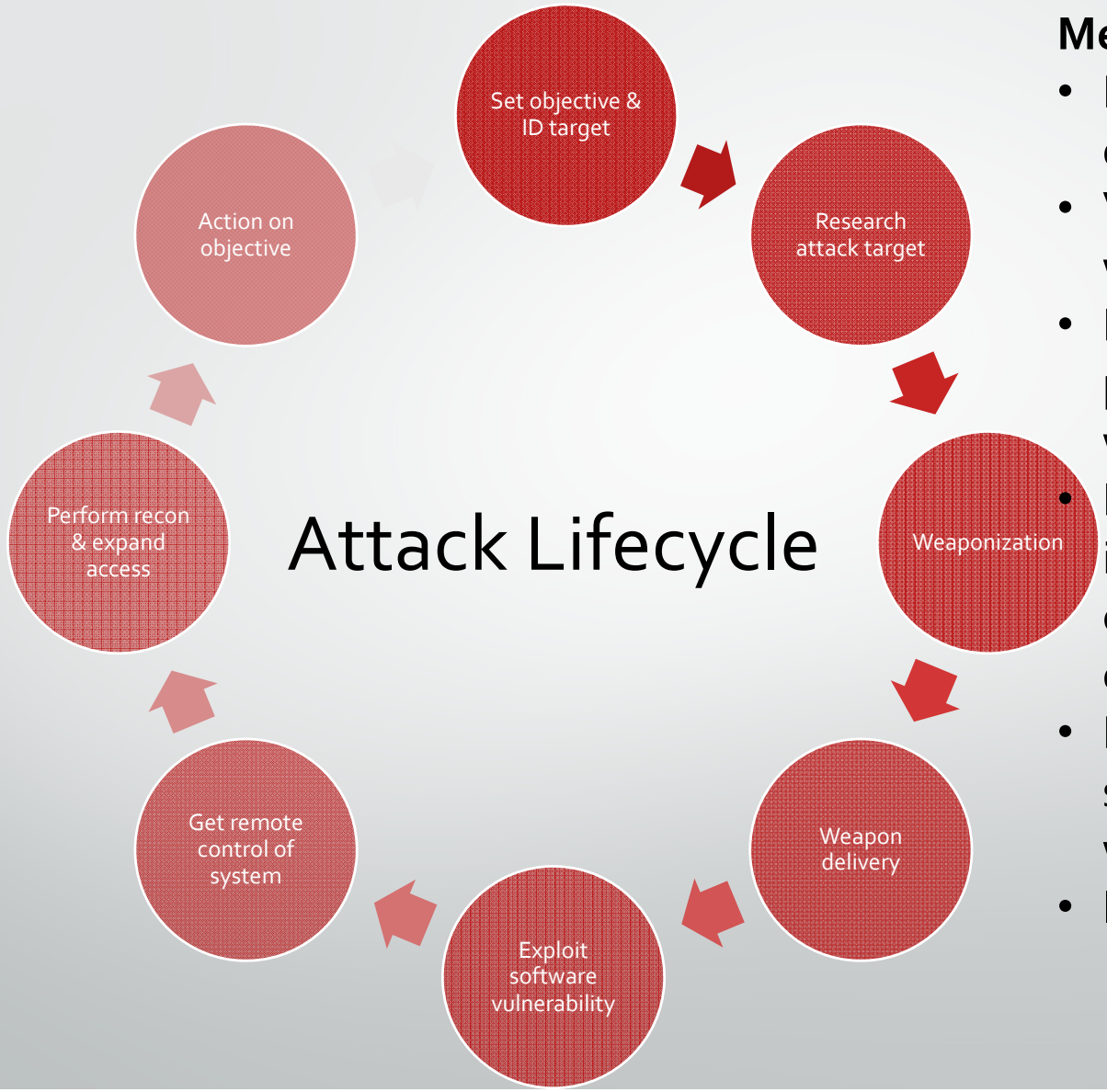
- **The Incident Response Plan**
- **Communicating the Data Breach**
  - **State law on notification**
- **You've Been Hacked/Attacked, What Are Your Next Steps?**
- The following are three steps to consider:
  - Triage/Evaluate the Cyber-event;
  - Invoke the Incident Response Plan; and
  - Review the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

DCCA HAWAII Division of Financial Institutions

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



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

DCCA HAWAII Division of Financial Institutions

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

DCCA HAWAII Division of Financial Institutions

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

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

DCCA
HAWAII
Division of Financial Institutions

What to do if you are the TARGET
STEP 2: Minimize Damage

- rerouting network traffic
- filtering or blocking a distributed denial-of-service attack or
- isolating 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

DCCA
HAWAII
Division of Financial Institutions

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

- a description of all incident-related events, including dates and times;
- information about incident-related phone calls, emails, and other contacts;
- the identity of persons working on tasks related to the intrusion;
- identity of the systems, accounts, services, data, and networks affected by the incident and a description of how these network components were affected;
- information relating to the amount and type of damage inflicted by the incident, which can be important in civil actions by the organization and in criminal cases;
- information regarding network topology;
- the type and version of software being run on the network; and
- any peculiarities in the organization's network architecture, such as proprietary hardware or software.

DCCA
HAWAII
Division of Financial Institutions

What to do if you are the TARGET
Step 4: Notify

- People in your organization
- 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

  808.586.2820
- Email: dfi@dcca.Hawaii.gov
- Twitter: @HawaiiDFI