Cyber Threats and the Role of the Auditor

Presented by:
Dale L. Rickard, CISA, CDP
IS Audit Supervisor
City of Colorado Springs

Stephen E. Coury, CISA
Chief Information Security Officer
The City and County of Denver

Mountain and Plains Intergovernmental Audit Forum
August 12, 2016

Session Abstract

As cyber threats continuously emerge, information security professionals are challenged to ensure that risks are managed and mitigated. At the same time, auditors are concerned that the cyber risk posture of the organization is properly recognized and reported.

This session will explore some real risks being faced by today's security professionals and offer discussion of what role auditors can take in these challenging times.

Learning Objectives:

- Gain awareness of emerging cyber threats.
- Consider roles that auditors can take in risk reporting

Hacking an Election

TION
US

THE HUFFINGTON POST
INFORM • INSPIRE • ENTERTAIN • EMPOWER

EWS POLITICS ENTERTAINMENT WELLNESS WHAT'S WORKING VOICES

THE BLOG

Top Six Ways Hackers Could Disrupt an Election

07/21/2015 12:32 pm ET | **Updated** Jul 21, 2016

510

Like 1.7K

Michael Gregg
COO, Superior Solutions

STOKKETE VIA GETTY IMAGES

http://www.huffingtonpost.com/michael-gregg/top-six-ways-hackers-coul_b_7832730.html

1. Voting Machine

- **Hack a voting machine -** The most obvious way to interfere with an election, of course, is by changing votes on an electronic voting machine. There are a number of ways this can be done, such as attacking the network the machines are being run on at a voting precinct, physically tampering with the device or the network hardware to install malware, attacking the voting machine company's network or employees to get malware into the devices or steal passwords before they are released to a government and target the back-end government network used to manage them. Hackers could also simply scan a government-run network to look for connected machines with default passwords.

2. Attack Agencies

- **Shut down the voting system or election agencies -** Similarly, hackers could use a distributed denial-of-service (DDoS) attack to disable voting machines or the back-end servers in order to deny access to voters. They could also launch DDoS attacks against local, state, and federal election agencies at key moments to disrupt voter registration, notification of voting precinct times and locations, record management, or coordination between agencies.

3. Election Records

- **Delete or change election records -** If you can breach a network, you can do almost anything you want to the data. Most of the time, we hear about hackers stealing or exfiltrating information - like the case of employee records at OPM. However, hackers could do something far worse - they could delete important data records, change the data or insert fake records. This would be particularly disastrous with election agencies. Imagine a hacker deleting voter registration forms to prevent people from voting, adding to the list of prohibited voters (like convicted felons), or switching a person's party affiliation to block him/her from voting in the proper primary. Or deleting a politician's filed paperwork, putting his/her candidacy in jeopardy.

4. Hijack Candidate Sites

- **Hijack a candidate's website -** Political campaigns often have lax cybersecurity, which, combined with a high rate of personnel churn and dependency on volunteer staff, makes it easy for hackers to infiltrate candidates' websites. There are a lot of ways a hacker could target a campaign website, such as DDoS'ing the site to deny access, installing malware to infect all visitors, or hijacking the Domain Name System (DNS) to redirect visitors to the wrong site which could expose them to malware or something offensive like pornography. In many cases, this would be more in line with harassment than a serious threat, but imagine how disruptive it would be to a candidate's campaign if he/she were forced to deal with technical issues constantly?

5. Doxing

- **Doxing a candidate -** Hackers could also take "mudslinging" to a whole new level by breaking into the candidate's, or staff's, private email accounts, smartphones, computers and any files or databases they've created in order to uncover sensitive and private information (as well as photos, videos, audio recordings) which could be publicly disclosed in order to damage the candidate. This practice of finding and revealing sensitive personal details is known as "doxing" in the hacker community, and it could be used to great effect in close elections. Attackers could also hijack social media accounts and post inaccurate or embarrassing information.

6. Campaign Donors

- **Target campaign donors -** There are also a lot of ways hackers could derail campaign fundraising. For example, since campaign contributions are public records, it would be easy for hackers to target commercial donors with DDoS and other attacks in order to discourage others from donating. They could also use SQL injection attacks on campaign websites to steal the credit card numbers of donors in order to harass them more directly, as well as engage in identity theft and financial fraud. But hackers wouldn't even have to go this far to affect a candidate's fundraising ability - simply announcing publicly that they planned to hack supporters might be enough to dissuade potential donors.

What is the Purpose of Audit?

- Yellow Book
  - Audits provide essential accountability and transparency over government programs.
  - Government auditing provides objective analysis and information needed to make the decisions necessary to help create a better future.
- Red Book
  - Audits provide an independent, objective assurance and consulting activity designed to add value and improve an organization's operations.
  - Auditing helps an organization accomplish its objectives by bringing a systematic disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance.

What Should Audit Do?

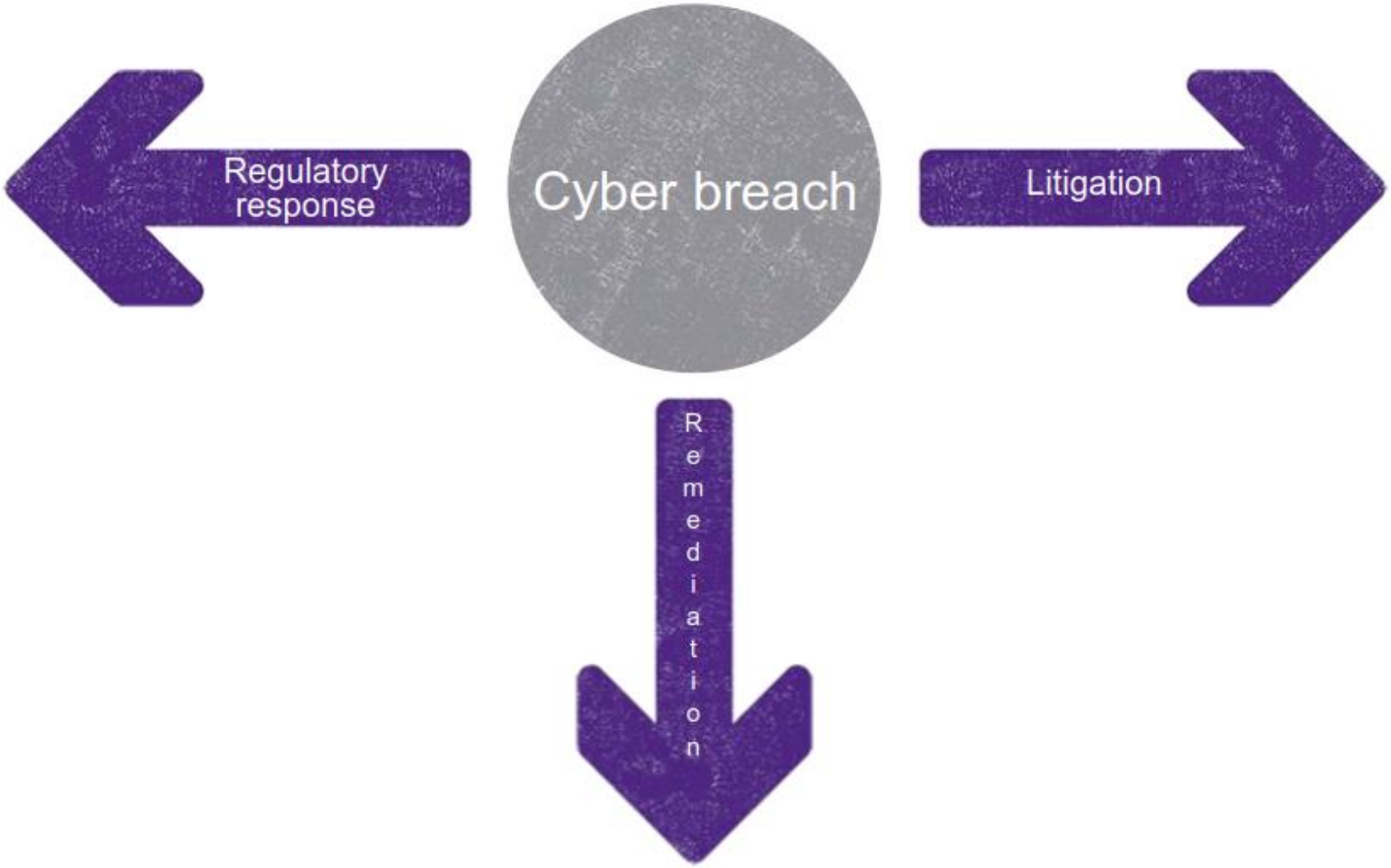
- Risk Assess
- Incident Response
- Business Continuity Plans

Why Risk Assess?

- Head in the sand approach no longer works.
  - In 2015, the average total cost of a data breach was US$3.79 million, up 23% since 2013[1].
- Good way to protect most technology assets is to unplug those assets from the network.
  - Not very practical today.
- Difficult to escape from technology in today's world.
  - Intranet, cloud, mobile, and social are mainstream platforms inherently oriented for sharing.
- Cannot protect everything.

[1]IBM & Ponemon Institute, *2015 Cost of Data Breach Study*

Why Understand Incident Response?



Why Understand Incident Response?

- Offenders often do not publicize their breaches.
  - Often claim credit once publically disclosed.
  - The longer the silence, the greater the value of the stolen data to those that did the breach.
- Gain an understanding of situational awareness.
  - How to deal with civil unrest?
  - How to deal with general rowdiness?
  - How to deal with public perception?
- Recovery most likely will “spoil” evidence.
  - Recover to alternate machines or facilities.
- Investigation most likely will delay systems recovery.
  - A detailed forensic investigation may take days.
  - Law enforcement may physically remove technology assets during the investigation.

Why Understand Business Continuity?

- What needs to be done if processing in the “cloud”?
  - Private cloud
  - Public cloud
  - Hybrid cloud
- What needs to be done if social platforms or accounts have been hacked?
  - Again, social platform is inherently oriented for sharing.
- Who, What, When, Where, Why, and How?
  - Who has to have the ability to do “stuff”?
  - What “stuff” absolutely needs to be done?
  - When does “stuff” need to be done?
  - Where does “stuff” need to be done?
  - Why does “stuff” need to be done?
    - Risk assessment
  - How is “stuff” going to get done?

How Should Audit Proceed?

- Ask Questions!!
  - Understand Management's Risk Assessment.
    - Has a Risk Assessment been conducted?
    - What are Management's risks as compared to the Board's risks?
      - How do these compare to Audit's risks?
  - Understand Management's Incident Response Procedures.
    - Has an Incident Response Team been created?
    - Does the Team have Management's support and authorization?
    - Is the Team conducting test responses?
      - Tests should be indicating what needs to be strengthened.
  - Understand Management's ability to meet Business Continuity.
    - Can Business continue to be conducted?
    - What Business needs to be conducted?

How Should Audit Proceed?

- Determine if in-house Expertise exists.
  - May need to acquire Expertise from External sources.
- Make Recommendations to better enhance any and all processes.

How Should Audit Proceed?

- How does one eat a whale?
  - One bite at a time.

Hacktivists Threats

https://www.youtube.com/watch?v=7tM2aEcjWJg

What Should Audit Do?

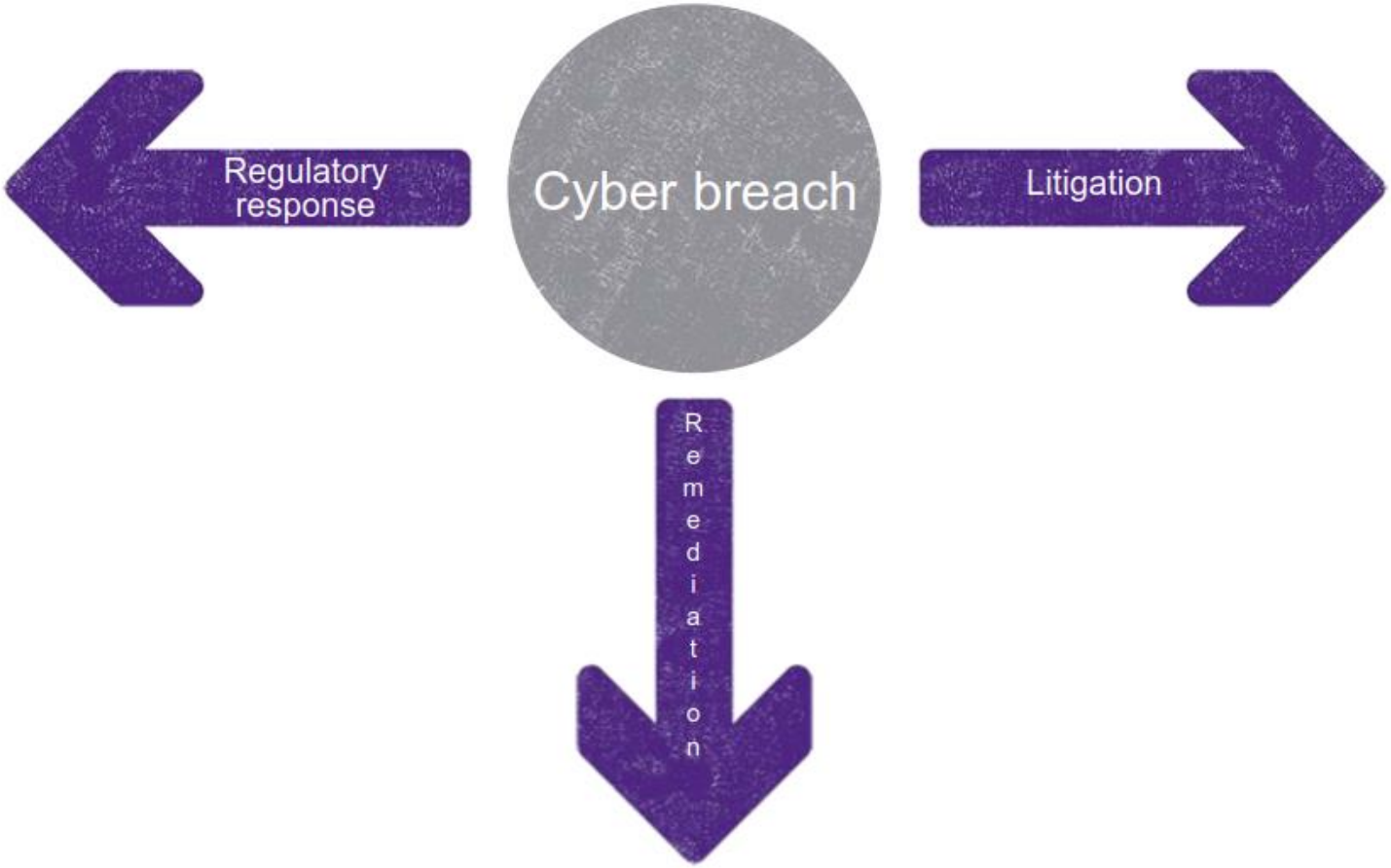
- Risk Assess
- Incident Response Procedures
- Keeping Informed

Why Risk Assess?

- Head in the sand approach no longer works.
  - Governments are the most attacked organizations in the world[1].
- Good way to protect most technology assets is to unplug those assets from the network.
  - Not very practical today.
  - Micro-segmentation of networks.
- Difficult to escape from technology in today's world.
  - Intranet, cloud, mobile, and social are mainstream platforms inherently oriented for sharing.
- Cannot protect everything.

[1]Federal Computer Week, 2016/Jul/27, *Dispelling the Myth of 'Perfect' Security*

Why Understand Incident Response?



Why Understand Incident Response Procedures?

- Audit can provide a role by assessing the organization's capabilities.
  - Does the organization have the necessary expertise?
  - Has the organization developed an Incident Response Team?
    - Management supported?
    - Authority of the IRT?
    - Testing of IRT responses to different situations.
      - Should be indicating areas that need to be strengthened.
    - Team members understand their roles and responsibilities?
  - Consult in the formation of the IRT.
  - Review cloud or outsourced resources contracts.
    - Adequate protection to the organization?

Why Keep Informed?

- Technology changes every day.
  - Quite often for the good.
  - Sometimes for the bad.
  - Audit needs to be aware of the use of new technologies.
    - Risk assessment.
- Management needs to keep as informed as Audit does.
- Unplugging from the network is not practical.
- Airplane mode is not practical.
- Living in a cave is not practical.
- Protecting everything is not practical.

How Should Audit Proceed?

- Do what auditors do best!
  - Ask questions!
- How does one eat an elephant?
  - One bite at a time!!