BerryDunn

Top Ten IT Security Risks: Data Breaches – Don’t Let Them Happen to You!

MAY 17, 2018

Presented by:
Chris Ellingwood, CISA, Senior Manager
Dan Vogt, CPEHR, PMP, Senior Manager

Goal

1 To describe the risks and types of breaches that CAP agencies are encountering.

2 Simulate an IT security incident and develop tactics for addressing.

Current Situation

- Breaches occurring with frequency
- Cyber-attacks have been monetized
- Incident preparedness is a challenge
- Limited available resources for addressing security
- Challenges continue to evolve

Agenda

1 Breaches & Risks

2 Mini Table Top Exercise

3 Wrap-Up

Takeaways

- Increase awareness of breaches
- Appreciate the need for practice
- Recognize the non-IT aspects

Breaches

“A **data breach** is the intentional or unintentional release of <u>secure</u> or private/confidential information to an untrusted environment.”

HTTPS://EN.WIKIPEDIA.ORG/WIKI/DATA_BREACH

Breaches

- ❑ 63% of not-for-profit organizations admit they have had a data breach in the last year

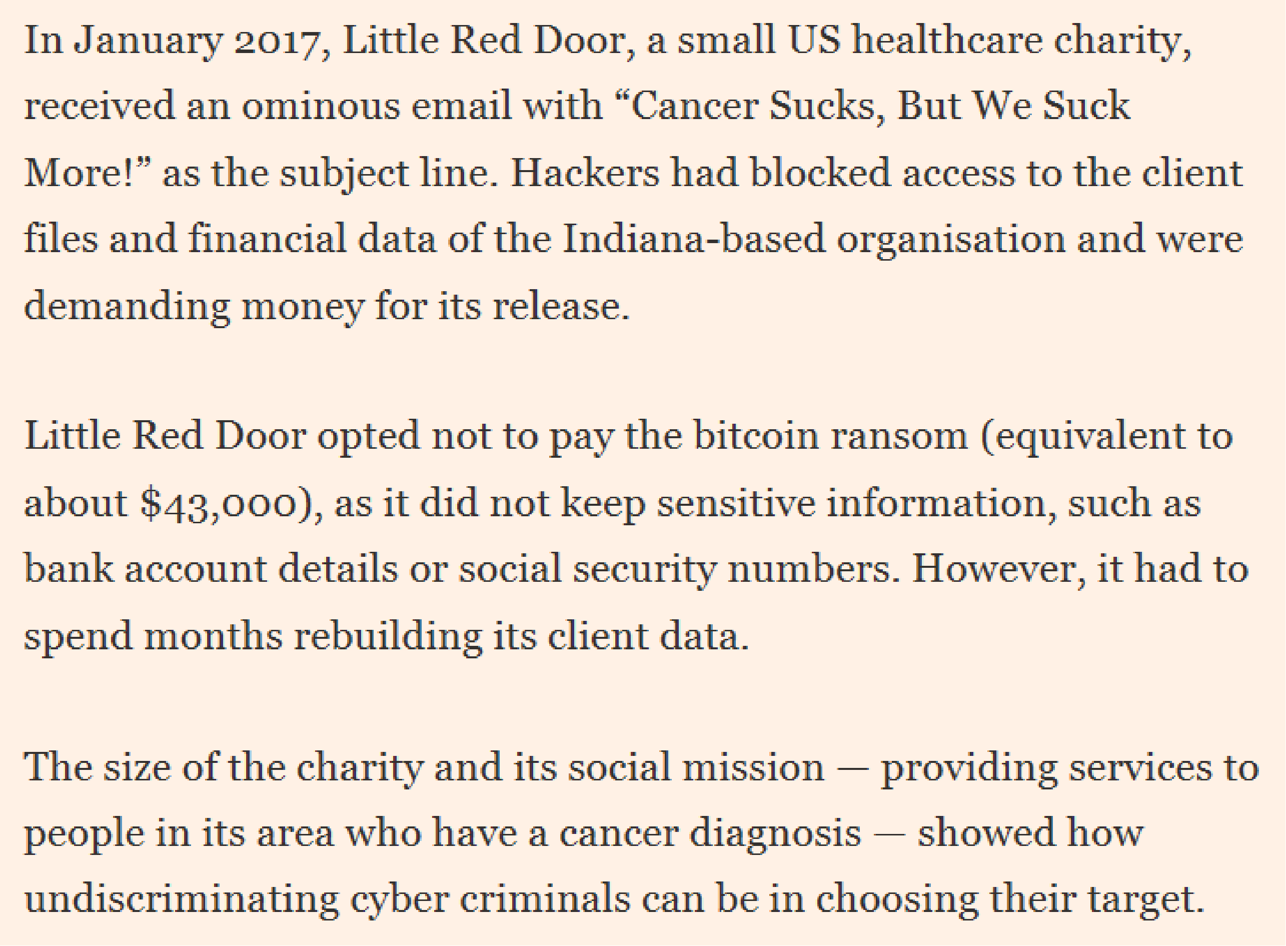
- ❑ 65% of the time, the root cause was something lost (laptop or paper file)

- ❑ Only 46% of the time, the breach was detected by IT

- ❑ 64% of the time, Compliance, Ethics, or HR departments led the response – NOT IT (only 18%)

http://www.corporatecompliance.org/Portals/1/PDF/Resources/Surveys/2016-data-breach-survey.pdf?ver=2016-12-12-073403-497

In the News



In January 2017, Little Red Door, a small US healthcare charity, received an ominous email with “Cancer Sucks, But We Suck More!” as the subject line. Hackers had blocked access to the client files and financial data of the Indiana-based organisation and were demanding money for its release.

Little Red Door opted not to pay the bitcoin ransom (equivalent to about $43,000), as it did not keep sensitive information, such as bank account details or social security numbers. However, it had to spend months rebuilding its client data.

The size of the charity and its social mission — providing services to people in its area who have a cancer diagnosis — showed how undiscriminating cyber criminals can be in choosing their target.

Breaches

CAP Data is full of targeted information by hackers

- Client Information
- May include personal data (birthdates, social security, etc.)
- Donor databases
    - used for phishing, on your behalf

Breaches

COST

COST EXAMPLES

- Investigation
- Remediation
- Identity monitoring
- Reputational
- Lost customers
- Equipment
- Legal
- Public relations

AVERAGE[1]

$225 per record

[1] PONEMON INSTITUTE – 2017 COST OF DATA BREACH STUDY

Breaches

WHAT CAUSES THEM?

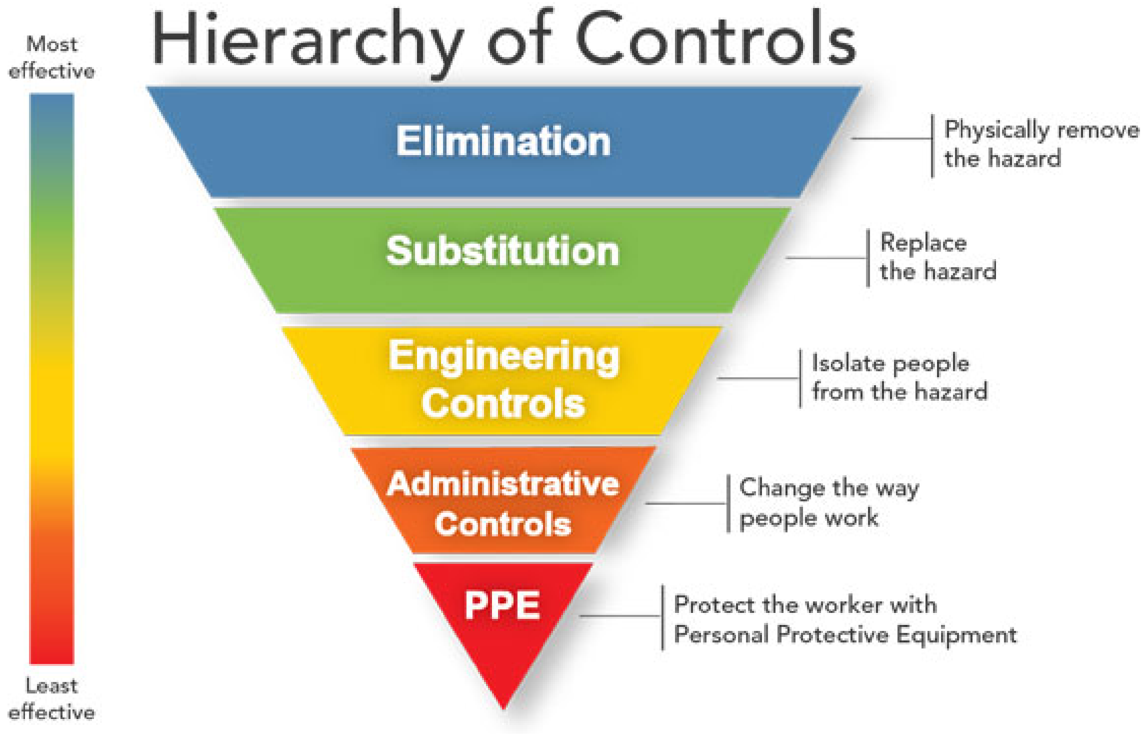
COMMON FACTORS

- Insider access/curiosity
- User carelessness
- Weak passwords
- Application and hardware vulnerabilities
- Elevated privileges
- Phishing

IMPACT OF THREAT × LIKELIHOOD OF OCCURRENCE = RISK

IT Risk

Controls are applied to identified risks to reduce the likelihood and impact


Hierarchy of Controls
Most effective
Least effective
Elimination
Physically remove the hazard
Substitution
Replace the hazard
Engineering Controls
Isolate people from the hazard
Administrative Controls
Change the way people work
PPE
Protect the worker with Personal Protective Equipment

Ten Risks

1. The Internet of Things (IoT)
2. Network Secured Only at Perimeter
3. **The World of Fakes**
4. Smartphone Hacking
5. Mergers and Acquisitions
6. **Lack of Data Classifications**
7. Cyber Insurance
8. **Phishing**
9. Lacking Risk Assessments
10. **Ransomware**

Four Added Factors

COMMUNITY ACTION PROGRAMS

1. Mission driven – to provide services
2. Limited resources (personnel)
3. Social media presence
4. Extensive networks

What Can You Do?

1. Conduct a risk assessment
2. Understand your data
3. Do the basics really well
4. Develop an incident response plan
5. Increase workforce awareness
6. Revisit your disaster recovery plans
7. Coordinate with your vendors
8. Conduct table top exercises

Mini Table-Top

Who are you?

1. Each table in the room is the management team of Ski Slope Partners
2. Ski Slope Partners is a CAP agency that supports the rural communities surrounding a world famous ski resort
3. The rural community has a poor economy, overshadowed by tourists and resorts
4. Your mission is to help the residents of the community obtain healthcare, transportation, and job training services

Who are you?

1. You have a central office team in the areas of finance, payroll, and procurement
2. You have one full-time IT Coordinator
3. Bob, a bookkeeper, is also tech-savvy and helps with IT
4. You use a third-party for the majority of your day-to-day IT needs
5. You rely on grants and fundraising
6. The community finds your services and learns of your mission mostly through social media

Fact 1

While sitting at your weekly management meeting your director of finance mentions that they have received emails from 4 of the 5 social workers working remotely describing unusual system slowness when trying to connect to office systems.

All of the business office staff are also complaining of a slow network and blaming your IT person for upgrading the system last night.

Fact 1

WHAT QUESTIONS DO YOU HAVE?

WHO DO YOU INVOLVE?

WHAT DO YOU DO?

Fact 2

After leaving the meeting you ask your IT Director and Bob to look into the slowness.

Bob receives an email from your IT third-party provider that they have detected malicious software running on a few of your servers.

These servers host your finance, client management, and payroll software.

Mary, your Community Outreach Director, also notifies you that she cannot log into Ski Slope’s Facebook page.

Fact 2

WHAT QUESTIONS DO YOU HAVE?

WHO DO YOU INVOLVE?

WHAT DO YOU DO?

Fact 3

After calling your IT support vendor and troubleshooting the server, your IT team lets you know that the malicious software is ransomware and your core systems are currently encrypted and data cannot be read by any end-users.

All of your social media accounts are also inaccessible and some well-known donors contact you to inquire about your “new” fundraising campaign. They are wondering why you are using a bank in Zimbabwe instead of your normal local community bank.

Fact 3

WHAT QUESTIONS DO YOU HAVE?

WHO DO YOU INVOLVE?

WHAT DO YOU DO?

Conclusion

Your IT team and support vendor were able to confirm that your backup was not affected by the ransomware and they were able to restore your systems from the 3am backup.

You reach out to your contacts and warn them of a potential phishing scam and to not respond.

Working with social media companies, you are able to take back control of your accounts and issue multiple press releases.

Your take the team out to dinner to celebrate!

Mini Table-Top

Fact 1

Mary, joyous from the triumphant recovery from ransomware and hijacked social media accounts takes a copy of your client and donor list on a thumb drive. She wants to spend some time over the weekend making sure everyone was properly contacted.

On her drive home she stops at Hannaford to pick up something for dinner.

Upon returning to her car she finds her windows broken and the thumb drive missing.

Fact 1

WHAT QUESTIONS DO YOU HAVE?

WHO DO YOU INVOLVE?

WHAT DO YOU DO?

Conclusion

Bob recently installed encryption software on all computers.

The encryption software requires all thumb drives to be encrypted before data can be saved onto them. A password must be entered to access the data.

Mary confirmed that she did use the software and created a strong password.

Conclusion

AGENDA

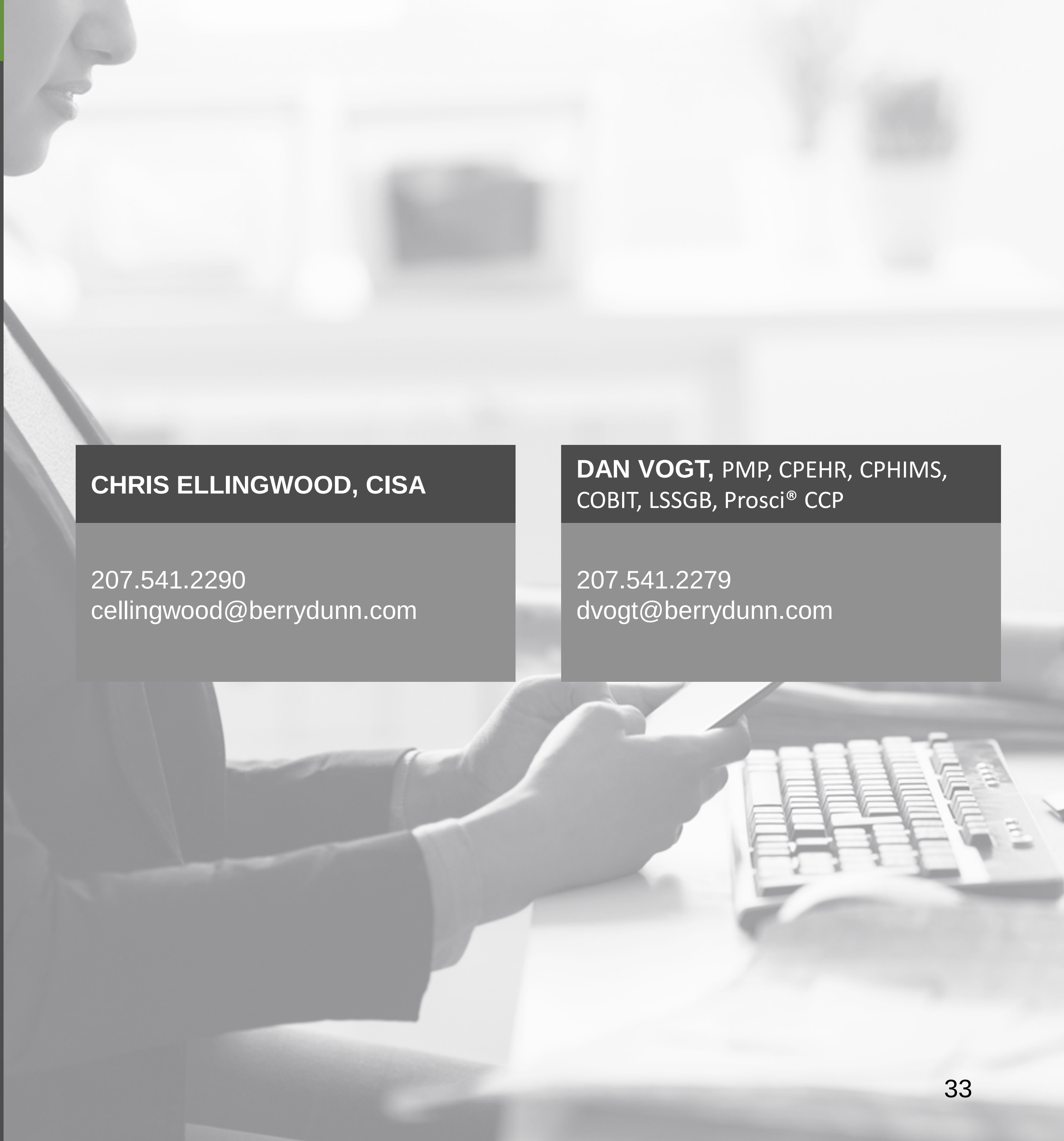
1. Breaches and Risks
2. Mini Table Top Exercise
3. Wrap Up

TAKEAWAYS

- Increase awareness of breaches
- Appreciate the need for practice
- Recognize the non-IT aspects

Questions

Contact Us



CHRIS ELLINGWOOD, CISA

207.541.2290
cellingwood@berrydunn.com

DAN VOGT, PMP, CPEHR, CPHIMS, COBIT, LSSGB, Prosci® CCP

207.541.2279
dvogt@berrydunn.com