Finance Professionals as Insiders
A Focus on Cyber Security Risks and Recommendations

May 9, 2019
Iowa HFMA

Michael W. Chase
Baird Holm LLP
It Happens To Everyone

Kindly Reply ASAP

Richard E. Putnam <57tqby694l@gmail.com>

You forwarded this message on 4/16/2019 7:01 AM. Extra line breaks in this message were removed.

Sent: Tue 4/16/2019 6:27 AM
To: Michael Chase
Retention Policy: BH-Apply to Inbox (3 years) Expires: 4/15/2022

Hello Michael,

I have a request I need you to handle before you get to work this morning please. Kindly Reply ASAP.

Thanks.

Richard E. Putnam
Look Familiar?

Invoice from Admin:

We removed extra line breaks from this message.

INV-21J0945865.doc
73 KB

Just catching up with back log and found the attached invoice, which I cannot find payment for??
I might have already sent this to you, if so apologies.
Remember This?

Patients diverted to other hospitals after ransomware locks down key software
Crypto-extortion increasingly targets bigger victims; most stay silent about it.

by Sean Gallagher - Feb 17, 2016 8:56am CST
Really? We're Still Talking About Ransomware?

• Health care industry is **still** under cyber attack (it's a goldmine)
• Industry experts are expecting the attacks to increase
• Cyber attacks and security incidents are getting more and more expensive
Ransomware $$$ Up

• All of 2015: $24M
  – Average demand: $295
• All of 2016 total: $1B
  – Average demand: $679
• 2017 average demand: $1,077
• 2018 average demand: $522
  • "High end" demands exceeding $15,000
Trending

• Business e-mail compromise (BEC)
• Ransomware and malware
• Cloud-based data breaches
• Mobile device exploits
Quick Update

• Digital transformation is underway
• Many organizations are embracing new technologies, including multi-cloud deployments
• Data environments are increasingly complex
• Each environment requires a unique data security approach
• In the end, much sensitive data is still at risk
Quick Update

• Advanced targeted attacks are persistent
• The attacks continue to be more and more sophisticated
• Target: individuals as the entry point
Insider Threat

- Ransomware and other malware part of a trend termed the “insider threat”
Types of Insider Threats

• **Malicious (Bad Actor)**
  A “Malicious Insider” make a conscious decision to intentionally commit theft or cause harm to an organization

• **Negligent**
  A “Negligent Insider” has awareness of a corporate data security policy, but chooses to ignore it (it’s inconvenient)

• **Inadvertent (Accidental)**
  An “Inadvertent Insider” makes a mistake and sends information to someone who should not have received it
What Do Attackers Want?

• Everything you've got!
  – Credit card/bank details
  – Protected health information (PHI)
  – Personally identifiable information (PII)
  – Trade secrets
  – Intellectual property
  – Credentials
Fraudsters Hard at Work

• There is an unprecedented amount of personal and sensitive information available
• Hacking tools are easy to access and design
• The attacks are becoming more and more sophisticated
• Looking for ways to monetize data through more targeted, wide-reaching attacks
• Low risk, high yield efforts
Where Does your Data Reside?

- Cloud-based?
- Hosted? By you? By vendor?
- Probably resides in structured databases, office documents, files, and...
E-mail, E-mail, E-mail

- E-mail is the gateway
- Think about it from the hacker's perspective
  - Easy to mine company databases, websites, social media, etc. to come up with the list of recipients
  - Easy to craft personalized e-mails that appear to be from a known, trusted source
Business E-mail Compromise

• HIMSS Survey: e-mail is the most common initial point of compromise for significant security incidents

• Why e-mail?
  – Scammers want credentials and other sensitive information
  – Once they're in, think about what's in your e-mail system (bodies of e-mails, attachments, etc.)
LinkedIn

Your LinkedIn account was suspended due to spam messages. To unlock your account open this link www.linkedin.com

Thank you for using LinkedIn!
The LinkedIn Team

Costco Shipping Agent <manager@cbobuilding.com>

Subject: Scheduled Home Delivery Problem
Date: January 6, 2014 10:54:37 PM MST
To:
Reply-To: Costco Shipping Agent <manager@cbobuilding.com>

Unfortunately the delivery of your order C06-0077945599 was cancelled since the specified address of the recipient was not correct. You are recommended to complete this form and send it back with your reply to us.

Please do this within the period of one week - if we don't get your timely reply you will be paid your money back less 21% since your order was booked for Christmas.
Phishing/Spam E-mails

• ~70% try to trick users into clicking on a malicious URL
• Malicious attachments also used
• Spam e-mail was the most common method for cyber criminals to spread malware in 2018
So You Clicked On The Link

• A ransom note appears – your files are encrypted and must pay a Bitcoin amount to decrypt the files
• Luckily, you've got a good backup policy and can promptly restore the system
• You know that most of your files (for example, electronic health records) are in a cloud-based application that was not affected by the ransomware
• So you activate your incident response plan
Incident Response

• How did the hackers get in the network?
• How long were they in the network?
• What did they access or exfiltrate?
• What did they do while in the network?
Were They In Your E-mails?

• Compromise of a single e-mail account could result in access to an entire network of sensitive information
  – Personally identifiable information (PII); protected health information (PHI); business plans/strategies; etc.
  – User credentials – for business and personal accounts
  – Also think about credentials for other systems (for example, cloud-based applications)
Were They In Your E-mails?

• Even if the attackers didn't gain access to the cloud-based applications (or credentials), what about your e-mail application itself?

• But – (and maybe you have policy) no one is supposed to use e-mail to send sensitive information (protected health information, personally identifiable information, etc.)

• Do you follow that policy internally?
Forensic Investigation of E-mail

• Now begins the hard part – was any of the information in your e-mails (and attachments) compromised?
• Begin a forensic investigation of your e-mail application
• What's unique about e-mail?
  – Unstructured
  – Attachments
  – Sometimes dual use (business/personal)
  – "Personal"
Forensic Investigation of E-mail

• Audit logging function can help in the post-incident forensic investigation process
  – It records almost every action
  – Was there an Office 365 login?
  – Was a document viewed?
  – Was a document downloaded or shared?
  – Was an e-mail forwarded?
  – Were settings changed?
  – Was the password reset?

• But…if the logs weren't turned on...
  – Or show that e-mails with attachments were automatically forwarded to an unknown, external e-mail address?
E-mail Breach Response

• Assume the account was compromised and everything within the account was compromised
• How are you going to review every e-mail (body text)?
• How are you going to review every attachment? What about those large spreadsheets with everybody's information?
• All within your regulatory/notification timeline?
E-mail Breach Response

• Luckily, there are vendors
  – Have developed algorithms and processes to search for PHI, PII, and other sensitive information
  – Also involves a manual review and logging of all the information (names, addresses, types of information)

• Of course, these services come at a high $$$

• Might be included in your cyber insurance policy
E-mail Breach Response

• Working with forensic vendors to unearth all of the e-mails, attachments, etc.
  – Do they know what they're looking for?
  – How will they log all of the information?
  – What does their work product look like?
  – **Can they get it done within your timeframe?**
    • Once they've found the information, the process isn't over
    • You've still got to complete the breach notification process (including finding last known addresses, etc.)
E-mail Breach Response
Lessons Learned

• While it is probably not feasible to prohibit the use of e-mail (for sensitive information) altogether, what should your policy be?
  – Minimum necessary amounts of info?
  – Use other applications such as secure file transfers?

• Log data can play a crucial role in the incident response
But I Don't Work In IT...
Cyber Security Isn't Only an IT Issue

• Keeping data secure is not the responsibility of only one department
• Preventing cyber attacks (and the resulting damage) is part of your world
• IT financing and budgeting are a part of an overall cyber security strategy
Cyber Security Isn't Only an IT Issue

• Cyber attacks are a costly problem
  – Notify affected patients/individuals
  – Security consultants (i.e., forensics)
  – Lawyers
  – OCR settlement or penalty
  – State agency settlement or penalty
  – Class action lawsuits
Cyber Security Isn't Only an IT Issue

• Invest in prevention
• Be an active part of the security risk analysis process
  – Make sure it happens (budget for it)
  – Identify the data and systems most likely to be hacked, the potential vulnerabilities, and the potential cost of disruption
• How are you going to budget for remediating vulnerabilities and gaps?
• You don't want an underfunded cyber security prevention program
Questions?
Questions?

Michael W. Chase
Partner
Baird Holm LLP
mchase@bairdholm.com
(402) 636-8326