CYBERSECURITY IN HEALTHCARE

Risks, costs, and protective measures

May 30, 2018
Presenters

Greg Vetter
Principal, Risk Advisory Services
Email: Greg.Vetter@rsmus.com
D: 212-372-1624

Lauren Winchester
Manager, Privacy Breach Response Services at Beazley Group
Email: Lauren.Winchester@beazley.com
D: 215-446-8417

Anthony Catalano
Director, Risk Advisory Services
Email: Anthony.Catalano@rsmus.com
D: 216-927-8223
Agenda

• Key NetDiligence findings
  - Interpretation and trend analysis
  - Changing threat landscape for healthcare

• Defending against cyber incidents
  - How are organizations getting compromised
  - Establishing a successful cyber program
    • Knowing which risks can transfer to a CLI policy
  - Incident response exercises

• Responding to a cyber incident
  - Leveraging your cyber policy
  - Common issues during and after an incident
KEY NETDILIGENCE FINDINGS
2018 Spotlight on healthcare

- Healthcare remains under attack
- Continued large losses in healthcare
High level findings

• While healthcare claims comprised 17 percent of claims in the overall 2017 claims data set, they represented 28 percent of total breach costs ($65 million of $229 million).

• The average total crisis services costs for healthcare was more than three times higher than the average for all other sectors ($676,000 vs $204,000).

• Credit and ID monitoring, and notification costs accounted for approximately 70 percent of healthcare breach costs.

• For example, RSM was able to compromise healthcare companies approximately 40 percent of the time during external penetration tests.
Key takeaways

• Approximately 63 percent of healthcare breaches were caused by criminal or malicious activity

• Few companies have more information, at a greater market value, on their customers than those in healthcare.

• Healthcare has improved its security posture in recent years and is generally average when compared to other industries.
  - However, the value of healthcare data remains relatively high
  - Healthcare organizations often pair healthcare and payment or financial data together.
Most prevalent attacks

- User awareness exploited more often than deficient technical controls
- Phishing is top overall attack vector
- Prevalent Windows vulnerability helps further extent of compromise
EMERGING THREATS AGAINST HEALTHCARE
Changing threat landscape – additional considerations

• Mobile device threats
  - As mobile devices continue to be used more and more, their relative exposure increases as well.
  - Virtually every employee, contractor, patient, and visitor to a medical facility has a mobile device on them, and many are likely connected to an internal wireless network.
  - It is critical to address and mitigate the mobile threat or healthcare might see even more incidents than predicted.
Changing threat landscape – additional considerations

- **Connected devices (Internet of Things)**
  - Hospitals and healthcare facilities are full of connected devices. In addition to connected infusion pumps, CT scanners, and patient monitors,
  - Increased complexity of IOT devices as well uses.
  - Outdates or nonexistent security in many devices.
  - We need to ensure these devices are updated, secured, and segmented.
2017 Healthcare incidents by cause

- Unintended Disclosure: 43%
- Insider: 17%
- Portable Device: 7%
- Hack or Malware: 21%
- Social Engineering: 3%
- Unknown: 1%
- Physical Loss/Non-Electronic Record: 8%

BBR Services 2017 Data
BEC – Vulnerability Linkage

Phishing email sent to CEO
- CEO opened attachment
- Attackers gained username and password

Attackers watched traffic
- Approximately two weeks
- Watched email style, nicknames, ongoing projects, and internal processes

Attackers sent internal emails
- 1st email to controller to set up a wire transfer
- 2nd email to procurement asking to pay vendor via wire transfer

Attack successful
- Controller and Procurement never questioned email or called CEO directly
Office 365 type attacks

- Record retention

Your mailbox is full.

2088/2560

Your SecureState mailbox has now significantly exceeded the limit assigned to you. Emails sent to you when your mailbox is in this state are not delivered and each sender should receive a notification of that fact. Please take action now to ensure that your mailbox is brought back under the limit.

What should you do?
Please login to your Outlook webmail via SecureState's portal here. Once logged in you will either need to delete any emails that you no longer need or archive emails that you wish to retain and then delete the originals.

Do you need more information?
We have some helpful information on the intranet regarding email settings. Follow this link: http://Intranet.SecureState.com.

SecureState Information Technology Department

This message is generated automatically by the server when you exceed the assigned capacity of your mailbox. Please follow the instructions in the email to resolve this issue or contact your network administrator.

- Outlook rules

Office 365

Your message from alldlcy@securestate.com couldn't be delivered.

A custom mail flow created by an admin at SecureState.com has blocked your message from alldlcy@securestate.com.

alldlcy@securestate.com Office 365

Action Required

Blocked by mail flow rule

How to Fix it

An email admin at SecureState.com has created a custom mail flow rule that blocks messages that meet certain conditions, and it appears as though your message has met one of these conditions.

Click here to view the message to make sure the message was not blocked by mistake.

More Info for Email Admin
Status code: 550 5.7.1 ETR

This error occurs because an email admin at SecureState.com has created a custom mail flow rule that has blocked the sender's message.

In some cases, the sender can change the message so it no longer violates the rule. However, depending on the rule's conditions, it's possible that the only way to deliver the message is to change the rule itself, and only an email admin at SecureState.com can do that. Although it's possible the rule is unintentionally flawed or it's stricter than the admin intended, it may be working exactly as they want it to.

Original Message Details
Created Date: 24/05/18 09:32
Sender Address: alldlcy@securestate.com
Recipient Address: alldlcy@securestate.com
Subject: Updates Made to Standard Operating Procedure

Error Details
BEING PREPARED FOR A CYBER INCIDENT
As many as 75 percent of U.S. hospitals responding to a poll could have been hit with ransomware in the last year, and a chunk of those might not even know it.

If hackers encrypted your hospital's patient data would you pay the ransom to get it back?

- Yes: 44.30%
- No: 50.80%
- Unsure: 4.90%

http://www.healthcareitnews.com/news/more-half-hospitals-hit-ransomware-last-12-months
Incident preparedness

• An IR tabletop exercise is the process of simulating an event to develop a high-level understanding of current cybersecurity processes, and how information, alerts and communication traverses the environment.

• This exercise becomes a critical success factor in the development and maintenance of a comprehensive, integrated, and security-focused response plan.
Training end users & vendor management

• Invest in training your employees.
• RSM recommends quarterly training and testing.
• Employees can be the weakest link or the first line of defense…
• **Free** tool to help organizations with this initiative.
• Vendor risk management portal
Considerations

• IT budgets are typically 3-7 percent of a company’s revenue, and security budgets are typically 5-8 percent of IT spend.
  - Assumed for a mature program, when “catching up” can go up to 30 percent

• Where is my next best security dollar spent?
  - Quantitative risk assessments.
  - Specific to business processes that are most critical.

• How are we measuring the success of our program weekly? Quarterly? Monthly?
How to work with your cyber carrier BEFORE a breach

• Elements to look for in a healthcare entity cyber policy
• Common coverage pitfalls
• What pre-breach, risk management services does your carrier offer?
• Gain an understanding from the cyber insurance carrier in advance to properly leverage your policy in the event of a breach
RESPONDING TO A CYBER INCIDENT
A breach alone is not a disaster, but mishandling it is.

Serene Davis – Underwriter with Beazley
How to work with your cyber carrier DURING incident response

• Key services needed during incident response
  - Legal
  - Forensics
  - Notification
  - Call center
  - Credit monitoring
  - PR and crisis management
  - Bitcoin payment and decryption assistance

• Costs of these services depends on size of incident
  - Forensic costs are usually highest, unless it is a very large incident
  - Mid-hundred thousands to millions of affected individuals, the notification, call center and credit monitoring costs start to exceed forensic costs
Board level discussion points

• When was the last time we practiced our cyber incident response capability?
  - What is my role in a particular incident?

• If an Incident happened right now could we continue operations?
  - Payment vs recovery

• What is OUR determined difference between a short term incident and a long term incident – as defined by the business?
  - Corporate environment vs subsidiaries

• How do we prevent issues from happening in the future?
  - Acting on documentation
How to work with your cyber carrier AFTER incident response

- Demands from affected individuals
- Lawsuits
- Regulatory investigations
- Regulatory fines and penalties
- Remediation