Shark Week: Understanding Cyber-Liability Insurance Coverage Issues

HALL RENDER
KILLIAN HEATH & LYMAN

HEALTH IT SEMINAR | INFORMATION TECHNOLOGY & DATA PRIVACY AND SECURITY

A SEMINAR FOR HOSPITAL AND HEALTH SYSTEM COUNSEL AND EXECUTIVES

SHARK WEEK

Understanding Cyber-Liability Insurance Coverage Issues

Presented by

Michael Rastigue, CISSP

Marsh Cyber Risk Practice

Stephen D. Rose, Esq.

Hall, Render, Killian, Heath & Lyman, P.C.

HALL RENDER
KILLIAN HEATH & LYMAN

Agenda

- Threat Landscape
- Protection
- Cyber-Liability Insurance

Threat Landscape

Cyber Criminals

POTENTIAL IMPACTS

- Data theft
  - → PII / PHI
  - → Banking information
  - → Cardholder data
- Cyber extortion
- Commodity malware
- SPAM

MOTIVATION

- Financial gain

Nation State

POTENTIAL IMPACTS

- Loss of intellectual property
- Destruction

MOTIVATION

- Cyber espionage
- National security
- Global competition

Hacktivists

POTENTIAL IMPACTS

- Data theft
- Reputational damage

MOTIVATION

- Fame and glory
- Ideological statements

Insider

POTENTIAL IMPACTS

- Data theft
- Reputational damage

MOTIVATION

- Disgruntled employee
- Financial gain

Cyber Terrorism

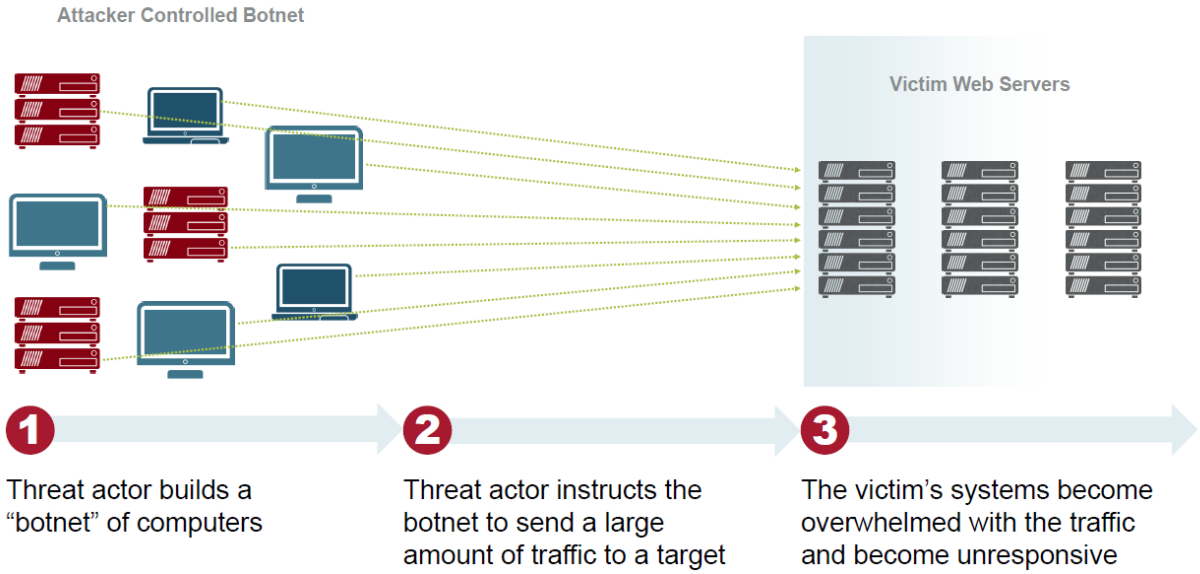
POTENTIAL IMPACTS

- Mass destruction

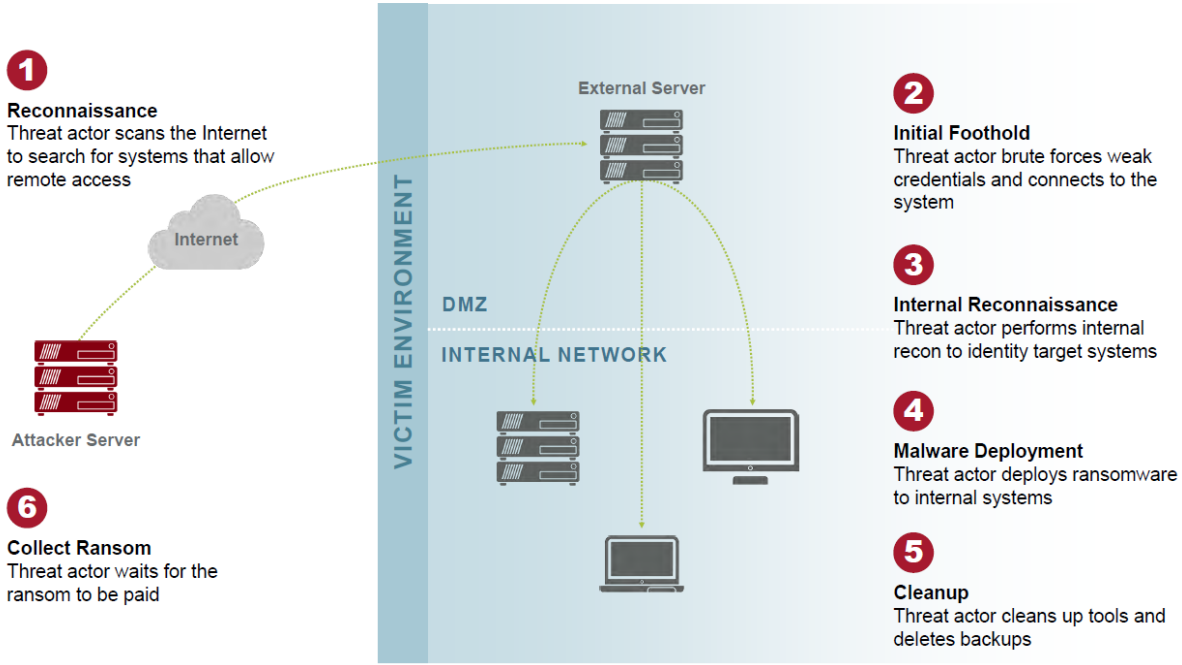
MOTIVATION

- Political or national interest

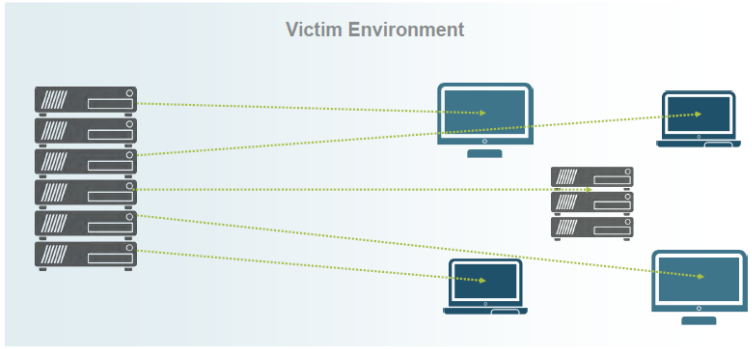
Anatomy of the Attack — DDOS



Anatomy of the Attack — Ransomware



Anatomy of the Attack — Targeted Destruction



1. The threat actor gains access into the internal environment through a phishing email
2. The threat actor gains administrative access to the rest of the environment
3. The threat actor executes malware on the system that permanently damages the system causing it to crash and make it impossible to boot again

How Can You Protect Your Systems?

1. Encrypt data
2. Manage ports
3. Train employees and create an Incident Response Team
4. Perform a Risk Analysis and Adopt Policies and Procedures
5. Know your business associates
6. **Transfer your risk—get insurance**

What Should Cyber Coverage Include?

Privacy Breach Response Costs: Patient Notification Expenses, and Credit Monitoring Expenses

- Should cover all reasonable:
  - Legal
  - Public Relations
  - IT Forensics
  - Call Center
  - Advertising
  - Identity Theft Education
  - Credit Monitoring
  - Postage

What Should Cyber Coverage Include?

Network Security & Privacy Insurance

- Coverage for third party claims alleging a financial loss as a result of a network security or privacy breach
- Should provide coverage for:
  - Virus attacks
  - Denial of service
  - Failure to prevent transmission of malicious code
- Covers both electronic and printed information
- Extends defense costs and coverage for fines and penalties under (but not limited to) HIPAA/HITECH, State Data Breach Laws and Red Flag Rules

What Should Cyber Coverage Include?

Network Asset Protection

- Coverage for all reasonable and necessary sums required to recover and/or replace data that is compromised, damaged, lost, erased or corrupted.
- Coverage triggered by Accidental, Unintentional and Intentional damage/loss/interruptions
- Includes coverage for Cyber Terrorism and IT Forensics
- Includes Business Interruption and extra expense coverage for Income Loss as a result of the insured's computer system interruption and/or failure

What Should Cyber Coverage Include?

Cyber Extortion/Ransomware

- Will pay extortion expenses and extortion monies as a direct result of a credible cyber extortion threat
  - Ransomware attacks are on the rise
    - Will continue to expand in severity
    - Average ransomware payment is increasing from a baseline of about $300-$500 per attack into the low thousands of dollars per attack
  - Assume ransomware attacks are foreseeable and will be more frequent

WannaCry

- Attack occurred May 12, 2017
- Thousands of companies affected
- Large percentage of companies affected were health care providers
- Why?
  - Health care providers possess large quantities of data rich information
  - Health care providers historically have been slow to protect data
- WannaCry continues trend of cyber-extortionists who lack the skills to create software needed for attack so just purchase ready-made programs

WannaCry


Wana Decrypt0r 2.0
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49
Your files will be lost on
5/19/2017 16:32:52
Time Left
06:23:59:49
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt
3 days ago

What Should Cyber Coverage Include?

Multimedia Insurance

- Coverage for both electronic and printed media
- Covers claims alleging:
  - Copyright/trademark infringement
  - Libel/slander
  - Advertising and false advertising
  - Plagiarism

Presenters

Mike Rastigue

MARSH

Vice-President Cyber Risk Practice

CURRENT RESPONSIBILITIES

Mike is member of Marsh's Cyber Center of Excellence where he advises some of the firm's largest and most complex clients about cyber risk. His clients span the Fortune 500, including defense contractors, healthcare providers, and critical manufacturers.

EXPERIENCE

Mike has brokered cyber risk insurance since 2011, for clients ranging from main street to the Fortune 10. Prior to joining the insurance industry, Mike ran a small IT consulting firm in Michigan.

EDUCATION

- CISSP (Certified Information Systems Security Professional)
- Juris Doctor, Western Michigan University Cooley Law School
- Bachelor of Arts, Philosophy, Oakland University

Presenters

Stephen D. Rose

Stephen Rose has more than 30 years' experience representing clients in the healthcare industry and serves as the Seattle Area Office Managing Partner for Hall, Render, Killian, Heath & Lyman.

His practice focuses on HIPAA/HITECH, Cyber Insurance Coverage, Medicare/Medicaid reimbursement, defending health care providers during government audits and responding to False Claims Act accusations.

HEALTH IT SEMINAR

INFORMATION TECHNOLOGY & DATA PRIVACY AND SECURITY

A SEMINAR FOR HOSPITAL AND HEALTH SYSTEM COUNSEL AND EXECUTIVES

Please visit the Hall Render Blog at http://blogs.hallrender.com for more information on topics related to health care law.

Michael Rastigue, CISSP
Marsh Cyber Risk Practice
312.627.6670
Michael.Rastigue@marsh.com

Stephen D. Rose
Hall Render-Seattle
425.278.9337
srose@hallrender.com