Advancing Healthcare Cybersecurity with Cyber Partnerships: *Ransomware Use Case*

Catherine Petrozzino, MS, CIPP/IT/G/US, cmp@mitre.org*

HIMSS Privacy and Security Committee Member

March 2018

**The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the author.*

Approved for Public Release;
Distribution Unlimited. Case Number 18-0506

Conflict of Interest

Cathy Petrozzino

Has no real or apparent conflicts of interest to report.

Educational Goal

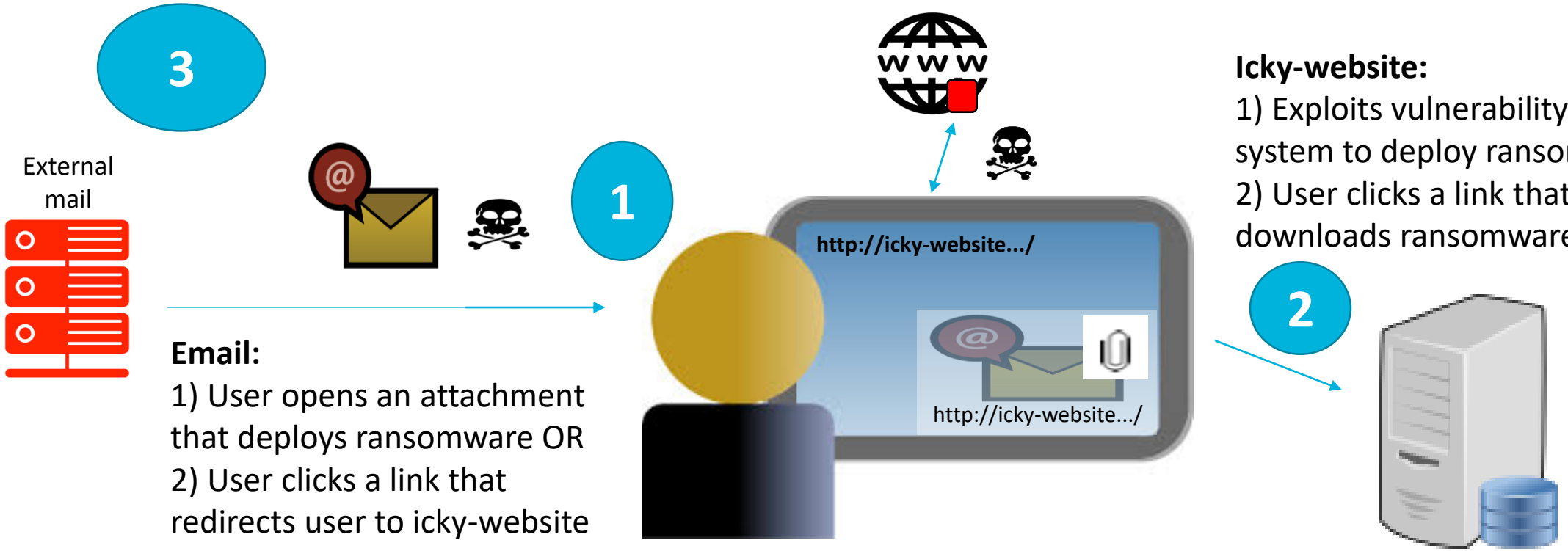
- **Identify available cybersecurity resources that can help elevate cyber defenses**

- **Identify organizations with cyber-oriented missions that are focused on assisting the broader community**
  - ‘Cyber partnerships’
  - Enjoy the fruits of others’ labors

- **Provide deeper insight and tactical assistance by grounding the information against a typical ransomware scenario**

Ransomware

- **Accounted for 72% of malware incidents in Healthcare during 2016***
- **Justice Department reported 4000 ransomware attacks *per day* in the first 9 months of 2016; only 13% of companies surveyed 'can prevent ransomware'****
- **Typically ransomware is deployed via e-mail or a web server**



Email:
1) User opens an attachment that deploys ransomware OR
2) User clicks a link that redirects user to icky-website

Icky-website:
1) Exploits vulnerability on user's system to deploy ransomware OR
2) User clicks a link that downloads ransomware

* 2017 Verizon Data Breach Investigations Report

**Ponemon Institute, The Rise of Ransomware, January 2017

Ransomware Risk Mitigation Opportunities

- **Securing the User** 1
  - Developing an Organization's 'Human Sensor' Network
  - Establishing a Culture of Security
- **Securing the System** 2
  - Configuring systems securely
  - Understanding the vulnerability landscape for a system
  - Staying aware of emerging vulnerabilities/malware
- **Securing the Organization** 3
  - Assessing gaps and implementing a security program
  - Building leadership buy-in

References Caveats

- **Include references and organizations with substantial free offerings**
  - There are commercial sites with free (basic) cybersecurity resources
  - Some commercial companies instrumental in standing up partnerships
  - Some non-profits sell their offerings
- **Starter list of available resources**
  - Exhaustive ⟶ impossible
  - Best ⟶ relative
- **Spread the love**
  - Smattering of content-rich web sites

1 Securing the User: Awareness

- **Tip Sheets and Foldouts**
  - Online Digital Advice for all Digital Citizens

    (https://**staysafeonline.org**/wp-content/uploads/2017/09/Online-Cybersecurity-Advice-for-All-Digital-Citizens-tip-sheet-NCSAM.pdf)
  - Ransomware Facts and Tips

    (https://**www.stopthinkconnect.org**/resources/preview/ransomware-facts-and-tips)
  - The Importance of Being EARNEST

    (https://www.mitre.org/sites/default/files/pdf/mitre_earnest.pdf)
- **Posters**
  - SANS Security Awareness Posters

    (https://**www.sans.org**/security-awareness-training/resources/posters)
    - Includes ’Protecting Healthcare Data’

1 Securing the User: Training

- **Educational Infographic**
  - Anti-phishing Page

  (http://phish-education.**apwg.org**/r/en/index.htm) - Anti-phishing Working Group

- **Video**
  - Cybersecurity for Small Businesses

  (https://www.**sba.gov**/tools/sba-learning-center/training/cybersecurity-small-businesses) - Small business administration

- **Smorgasbord (videos, games, information)**
  - FTC Onguard Online Campaign

  (https://www.consumer.**ftc.gov**/features/feature-0038-onguardonline) - Federal Trade Commission

2 Securing the System: Secure Configurations

- **Benchmarks – Secure configuration of (common) operating systems and applications**
  - Configuration guidelines

  (https://www.**cisecurity.org**/cis-benchmarks/) – Center for Internet Security
  - Automated benchmark tool

  (https://learn.cisecurity.org/cis-cat-landing-page)

- **Vulnerabilities – Known weakness that can be exploited in a system**
  - National Vulnerability Database

  (https://nvd.nist.gov/)
  - Common Vulnerabilities and Exposures (CVE)

  (http://cve.mitre.org/)

2 Securing the System: Alert Mechanisms

- **Bulletins, Alerts, Activities**
  - United States – Computer Emergency Readiness Team (US-CERT)

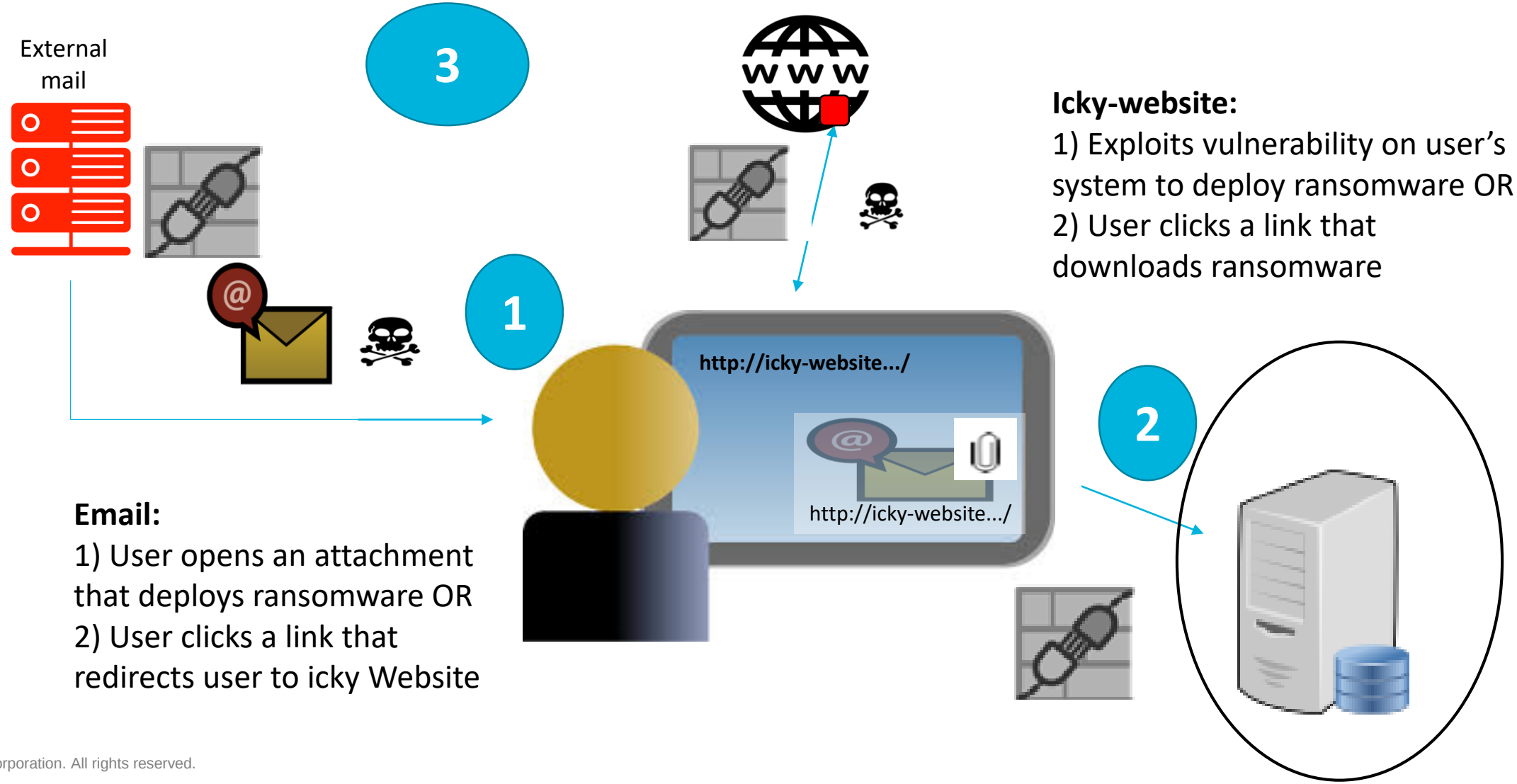
    (https://www.us-cert.gov/ncas)
    - Recent security updates, vulnerabilities, malware
    - Also has a tips section with lots of tactical guidance
  - Industrial Control Systems – Cyber Emergency Response Team (ICS-CERT)

    (https://ics-cert.us-cert.gov/)
    - Applies to critical infrastructures, which includes healthcare
    - ICS-CERT has reported on medical device vulnerabilities

    (US-CERT and ICS-CERT run by DHS; subscription service is available)
  - No More Ransom Prevention Advice

    (https://www.**nomoreransom.org**/en/prevention-advice.html)

Ransomware: Potential Organizational Controls



Icky-website:
1) Exploits vulnerability on user's system to deploy ransomware OR
2) User clicks a link that downloads ransomware

Email:
1) User opens an attachment that deploys ransomware OR
2) User clicks a link that redirects user to icky Website

3 Securing the Organization: Assessment

- **Assessment tools**
  - HIPAA Security Assessment Tool

    (https://www.**healthit.gov**/providers-professionals/security-risk-assessment-tool)
  - NIST Cybersecurity Assessment

    (https://www.nist.gov/sites/default/files/documents/2016/09/15/baldrige-cybersecurity-excellence-builder-draft-09.2016.pdf)
- **Implementation**
  - NIST Risk Management Framework

    (https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides)
  - CIS Controls – identifies the most critical enterprise security controls

    (https://www.cisecurity.org/controls/)

3 Securing the Organization: Leadership

- **Tip Sheet**
  - Communicating cyber to the board

(https://**staysafeonline.org**/wp-content/uploads/2017/09/Communicating-with-the-Board-about-Cybersecurity-Making-the-Business-Case.pdf)

- **Cyber and Privacy Breach and Cost Studies**
  - Sixth Annual Benchmark Study on Privacy and Security of Healthcare Study (May2016)

https://www.**ponemon.org**/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf

  - 2017 Cost of Cyber Crime Study

(https://www.ponemon.org/library/2017-cost-of-cyber-crime-study)

  - The Rise of Ransomware, January 2017

(https://www.ponemon.org/local/upload/file/Ransomware%20Report%20Final%201.pdf)

The Top 3 ”Cyber Partnerships”

- NIST (www.nist.gov)
  - Detailed, comprehensive cyber guidance
  - National Cybersecurity Center of Excellence (NCCoE, nccoe.nist.gov) developing Practice Guides (1800 series) built around Use Cases
- DHS (www.dhs.gov)
  - Offers vast array of cyber insights at different levels as well as vulnerability and threat information
- HIMSS
  - Many healthcare related resources linked through the privacy and security toolkit
  - Operate the healthcare cybersecurity community
  - Generate a monthly cyber highlights newsletter

Questions?