SecurityScorecard

Bridging the Gap Between Privacy and Security

Fouad Khalil
Head of Compliance

Tuesday March 27th, 2018

What's the difference between privacy and security?

PRIVACY: The principles and rules that govern how health information is protected and kept confidential

SECURITY: The confidentiality, integrity, and availability of data, networks, and systems

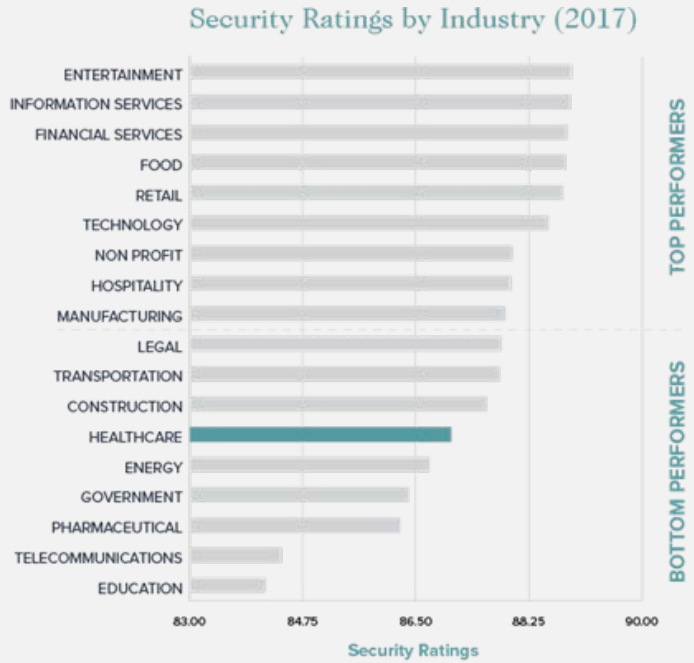
2018 Brings More Cybersecurity Risks And Uncertainty: Is the Healthcare Industry Ready?

Healthcare Industry: Key Insights

- The healthcare industry ranks fifteenth in terms of cybersecurity health when compared to seventeen other major U.S. industries.
- The healthcare industry is one of the lowest performing industries in terms of endpoint security.
- Social engineering attacks continue to be a common attack vector.
- The most common cybersecurity issues in the healthcare industry relate to poor patching cadence.
- Healthcare organizations, even top performers, struggled with patching cadence and network security.

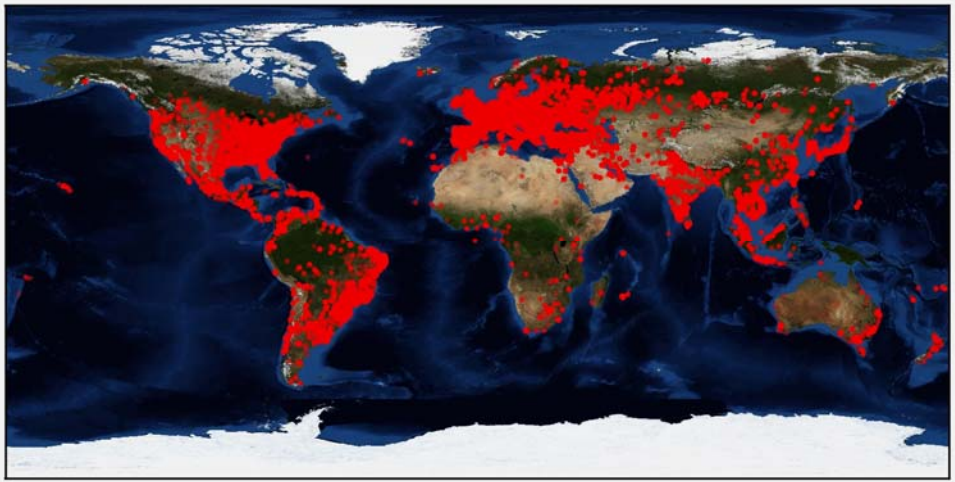
Healthcare Industry: Facing An Uphill Battle

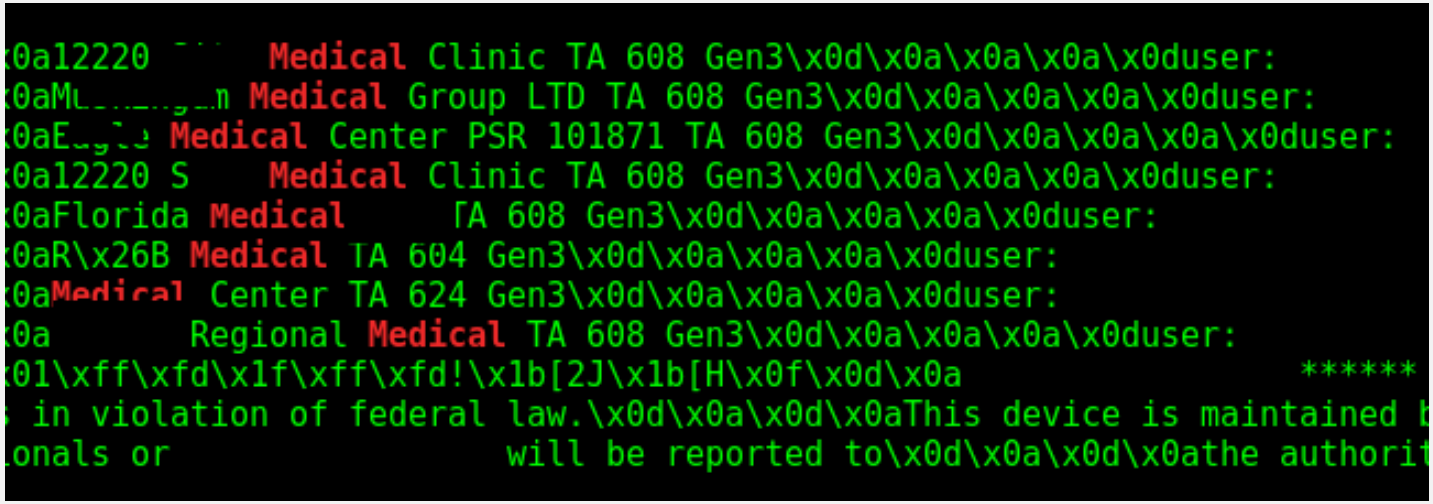
- ***Healthcare lags in cybersecurity performance*** when compared to other industries.
- ***… and the industry has recently dropped to 15th from 13th.***

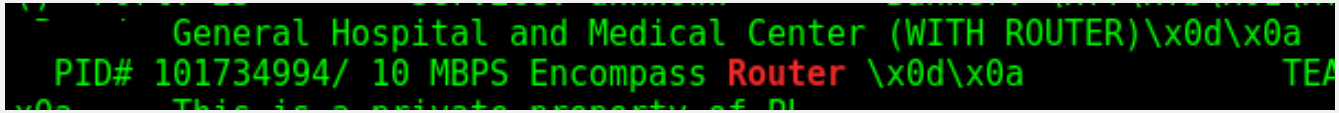


One example: IoT Landscape Posing Increased Risks

- SecurityScorecard ran a scan on over 200,000 IoT devices and found many that were vulnerable- i.e. in the case of healthcare organizations, hackers can get access to PHI.
- ***Healthcare companies*** owned some of these devices.

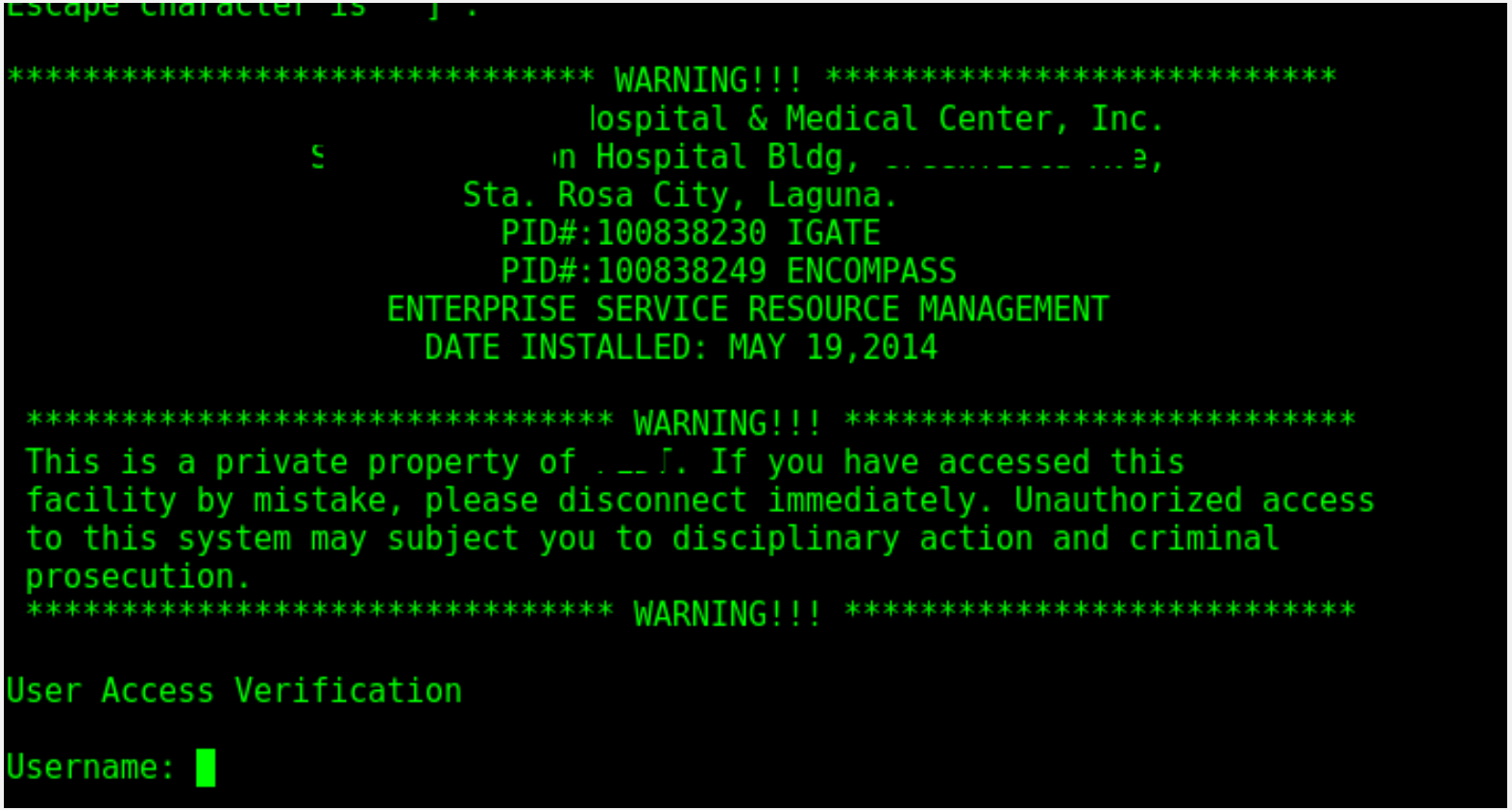






Not only is the healthcare industry making use of legacy routers exposed to public internet, we see information about the hospital using these routers.

Example of warning message from legacy router.



Why unify privacy and security initiatives?

- Highly regulated healthcare organizations have limited resources for achieving and ensuring continuous compliance with evolving HIPAA regulations.
- Consolidating privacy requirements and security controls allows health providers to streamline compliance activities and optimize resources.
- Assessing, monitoring, and reporting on privacy and security requirements via one centralized portal enables instant visibility of critical information and facilitates consistent HIPAA compliance.
- HIPAA compliance requires adherence to the HIPAA Privacy Rule and the HIPAA Security Rule. One fails without the other.

Healthcare Privacy & Security Challenges

Current State of Healthcare Cybersecurity

•96% of all ransomware attacks last year targeted medical treatment centers.*

•An estimated 4.5 million electronic health records were exposed last year.*

•89% of healthcare organizations had at least one data breach involving the loss or theft of patient data in the past two years.****

•Data breaches cost the U.S. healthcare industry more than $6 billion a year.**

•Healthcare organizations allocate less than 6% of IT budgets for cybersecurity.***

•Privacy and security budgets have decreased or stayed the same.****

•Regulatory restrictions governing use, storage, and process of personal information are increasingly stringent in the healthcare sector.

•Trust and safety are paramount in healthcare; a cyberattack damages provider credibility and reputation.

•System compromise and disruption of care may have devastating impacts on patient health.

*SecurityScorecard 2018 Healthcare Industry Cybersecurity Report
**Ponemon Institute
***Symantec
****Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data (Ponemon Institute 2016)

Elements of a Weak Healthcare Cyber Defense

- It takes healthcare systems months to discover nearly 40% of all data breaches.* It typically takes cybercriminals only minutes to compromise health provider infrastructure and steal patient records.
- Personal health information is a lucrative commodity on the black market. Medical records contain the valuable data hackers want… name, address, social security number, credit card information… for identity theft and fraud.
- Multiple healthcare providers access confidential information to ensure continuity of care for individual patients. Digital information workflows, increased connectivity, the proliferation of mobile devices, and use of cloud services are expanding the modern attack surface.
- A shortage of skilled health IT and cybersecurity professionals, constrained budgets, nonexistent or unenforced security policies, and a lack of cyber risk awareness and understanding of the threat landscape contribute to industry vulnerability.
- Continued reliance on outdated and unsupported (unpatched) legacy systems, misconfigured devices, vulnerable IoT medical devices, lack of continuous threat monitoring, and fragmented infrastructure vulnerable to data leaks and cyberattacks result in obsolete defenses that are no match for today's hackers.

*Verizon Data Breach Report

Recommendations

Adopt Best Practice Privacy and Security Controls

Implement policies and procedures to:

- Prevent, detect, contain, and correct security violations.
- Ensure all members of workforce have appropriate access to ePHI.
- Authorize access to ePHI.
- Rapidly and effectively address security incidents.
- Control access to electronic information systems that maintain ePHI.
- Record and examine activity in information systems that contain or use ePHI.
- Protect ePHI from improper alteration or destruction.
- Verify identities of those seeking access to ePHI.
- Guard against unauthorized access to ePHI transmitted over electronic communications networks.

*Verizon Data Breach Report

Rely on a Single Platform to Manage HIPAA Compliance

- Deploy advanced security tools and technologies that map directly to HIPAA Privacy *and* Security rules.
- View privacy and security data on one dashboard for an instant snapshot of real-time compliance status.
- Continuously track HIPAA compliance adherence and detect potential gaps.
- Capture, report, and remediate contractor, vendor, and partner security risks that signal potential violations with regard to protecting patient information.
- Automate third-party compliance to instantly assess and always know the security posture off all service provider partners in your ecosystem.
- Continuously assess and analyze risk across ecosystem to protect the confidentiality, integrity, and availability of ePHI.

Embrace the Benefits of Comprehensive Ecosystem Risk Management

- Secure health systems, medical devices, and patient data across the healthcare organization ecosystem.
- Gain the visibility, intelligence, and insight needed to act on emerging cyber threat data, proactively protect private patient information, and improve the cyberhealth of your organization and ecosystem.
- Discover, monitor, and report on the security posture of your organization as well as any service provider partner.
- Eliminate data asset vulnerabilities before attackers exploit them.
- Improve cybersecurity awareness and readiness to prevent predictable breaches and data loss.
- Improve efficiency while ensuring continuous compliance with HIPAA Privacy and Security rules.
- Easily achieve, confidently prove, and continuously maintain compliance while eliminating reporting headaches and minimizing risk of penalties.
- Leverage HIPAA privacy and security compliance to reduce the risk of a data breach that could cause reputation damage and/or jeopardize patient health.

Unify Privacy and Security Efforts to Streamline Compliance and Reduce Risk

- Increased breach risk requires greater due diligence in protecting confidential patient information.
- Ensuring continuous regulatory compliance is a critical element of risk mitigation. Sustained HIPAA compliance helps safeguard patient information and reduce the risk of data breaches.
- Proving HIPAA compliance requires continuous monitoring and enforcement of best-practice security controls across your entire ecosystem, including all contractors, vendors, and partners.
- A cultural shift is required to recognize that quality healthcare delivery extends beyond treatment services and must include robust cybersecurity practices to ensure patient safety.

*"Healthcare cybersecurity is a key public health concern that needs immediate and aggressive attention."**

*Health Care Industry Cybersecurity Task Force Report (June 2017)

SecurityScorecard

Thank You

Fouad Khalil
Head of Compliance

info@securityscorecard.io

214 West 29th St, 5th Floor
New York, NY 10001