CHART
Center for Health Analytics, Research & Transformation at NJHA

BULLETIN

Cyber Security is Critical to a Culture of Safety

Cyber security affects everyone. Businesses, government agencies, and individuals have a responsibility to protect themselves and other parties they interact with in the digital space. Protecting oneself from viruses, malware, and hackers begins with understanding the risks. But true security requires an organization to make cyber vigilance part of its culture.

Any computer, cell phone, or tablet contains coveted information such as e-mail addresses, names, birth dates, pass codes, and text messages. Any information connected to a smart device can be accessed through a breach in security. A personal device could include social security numbers, tax records, bank records, and credit card information.

In the healthcare realm maintaining data integrity is critical. In the healthcare environment, this might also include personal health information. Malware can corrupt, alter, or steal patient records, lab results, allergy information, and drug interaction histories, affecting patient care.

All it takes is for one employee to knowingly, or unknowingly, do something that exposes the organization – click a bad link, lose a device, or open a malicious attachment. Patient data is targeted by hackers because it is valuable. Patient data including name, birthdate, insurance policy number, diagnosis codes, and billing information, is sufficient enough to create a fake identity, file false insurance claims, make illegal purchases, identify personal vulnerabilities to extort, and to even file a false tax return.

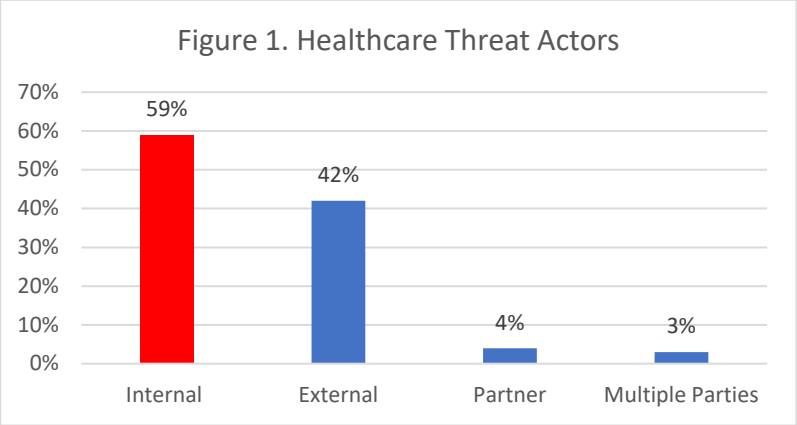
While chief information officers and chief information security officers are well aware of the threats that a cyber-attack may have on healthcare organization, the magnitude and dangers associated with patient care disruption make the importance of top leadership's involvement in cyber security more apparent than ever. Recently published news reports of serious cyber incidents serve as a reminder to healthcare leadership that these threats are real and are increasing in frequency, with greater operational impact. Cyber-attack related disruptions to routine patient care is clear evidence that cyber security strategies and defenses are important components of an organization's culture of patient safety.

Landscape of Cyber Security and Healthcare

Healthcare organizations represent a small percentage of the cyber security incidents in the nation, but the impacts of healthcare breaches are expensive and dangerous. The 2019 Data Breach Investigation Report by Verizon indicates that 81 percent of the threats within healthcare were due to "Miscellaneous Errors, Privilege Misuse and Web Applications." Verizon's report identified 59 percent of the cyber threats in the healthcare sector as being from internal actors, meaning that employees of the organization are not taking vulnerabilities seriously. The report cites phishing emails as a very common scenario for duping users, along with other unintentional mistakes.

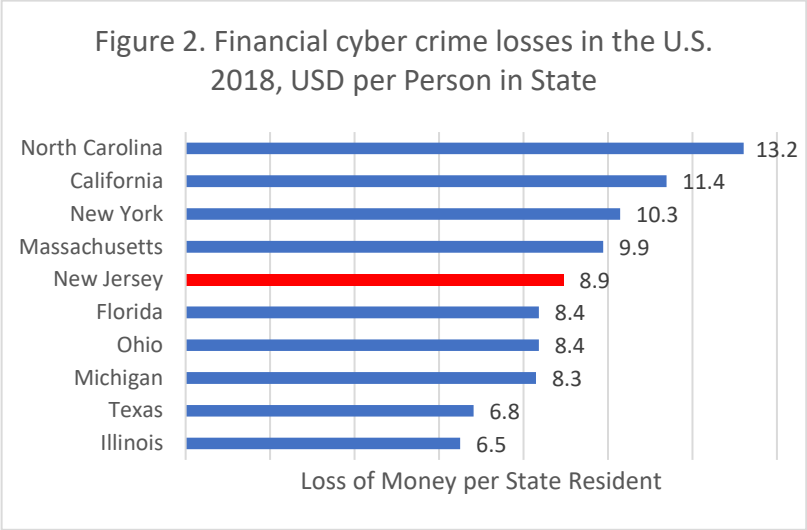
The healthcare sector is a very dynamic, fast-paced, and stressful environment, leaving room for human error in securing data. When one considers that 72 percent of the data compromised in healthcare security breaches involve medical data and 34 percent involves personal data, it makes cyber security challenges even more dire.

To health! NJHA New Jersey Hospital Association



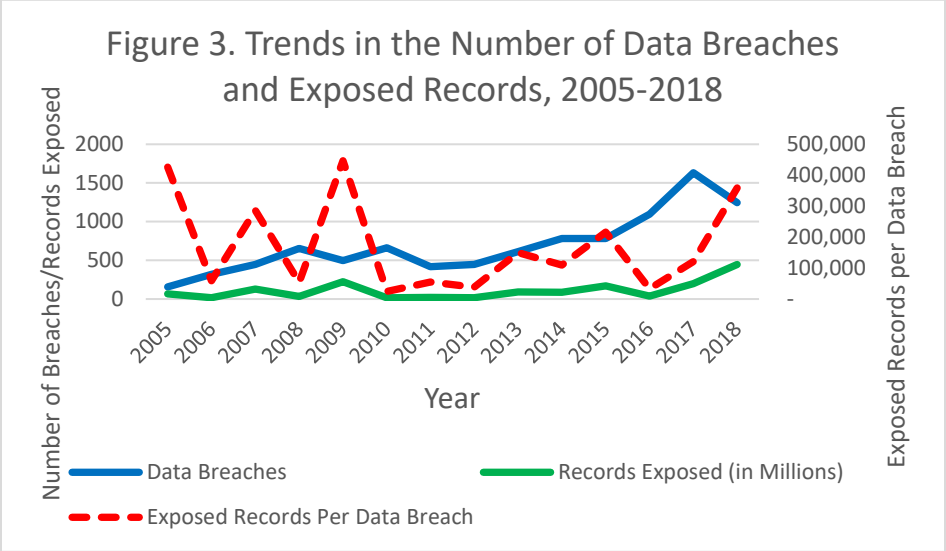
Source: *Verizon, 2019 Data Breach Investigations Report*

Financial losses associated with cyber crimes can be substantial. According to a report by Statista, North Carolina ranks first in the country with a per capita loss of more than $13 per person or $137.2 million total in 2018 alone. By comparison, New Jersey ranks fifth among states with a per capita loss of nearly $9 per person or $79.7 million annually.



Source: *Statista, U.S. Consumers and Cyber Crime*

Despite increased awareness in protection and detection, the number of data breaches have been rising steadily since 2012. The number of exposed records per breach has also increased since 2013 (Figure 3).



Source: Statista, *U.S. Consumers and Cyber Crime*

Steps a Healthcare Organization Can Take

Clinical practitioners know that a culture of safety means taking the time to do the small, everyday actions that add up to keeping patients healthy. Mundane tasks like keeping carts stocked, going through checklists, and consistent hand hygiene all play a role when a patient's safety is concerned. Similarly, healthcare organizations that incorporate good cyber security hygiene into their culture better protect their patients' and organization's data.

According to healthcare security experts, organizations can take specific actions to thwart a cyber-attack. The three basic strategies are:

Patch and Update Systems. This includes operating systems, virus protection, medical devices, mobile devices, network hardware, and any applications operating within the infrastructure or connecting to the organization.

Educate the Workforce. Employees need to be continuously educated and made aware of the cyber security threats that could impact themselves and their patients. Cyber security is not just the role of the information security team – it's part of everyone's job.

Simulate. Organizations should simulate phishing and even larger scale cyber-attacks. Employees will realize that, even if attacked, there are strategies that can be deployed to minimize impact or continue operating under a Plan B. Simulating phishing attacks are the best way to gauge employee awareness and are an excellent education opportunity.

Recognizing that healthcare data is a prized target, healthcare organizations should also conduct an annual risk assessment as required under HIPAA. This requirement helps healthcare organizations identify strategies to mitigate risk. If done properly, this can establish preventive measures to avoid future problems.

Defending Your Organization

Just as when organizations implement quality improvement projects, incorporating cyber security into the culture of an organization requires buy-in and engagement from top leaders. Empowering information technology teams to implement best practices, study outcomes, and react to the ever-changing threats to data security will enhance resiliency and deter potential bad-actors.

Organizations may not be able to predict every type of possible attack, but the need for information technology security staff to get continuous education on the latest cyber threats is critical. Conducting reality based annual risk assessments informed by newly emerging threats is critical to an organization's security defenses.

As cyber-attacks continue to evolve and get more complex, so do technical systems defenses. Today, most organizations run a myriad of security applications designed to prevent and detect a cyber intrusion. In addition to monitoring outside attempts to access an organization's network, some services are able to alert security staff when internal software is inappropriately communicating with outside entities. Existing technologies have also grown in their abilities to secure networks; for example, modern firewalls are able to detect and block internet traffic from foreign countries. Knowledge of an organization's current security product's abilities and limitations to defend against a new threat is very important.

Resources

To address growing cyber threats, there are a number of resources available at both the state and federal level. They provide the latest threat intelligence and help organizations that are dealing with real-time cyber security incidents.

In New Jersey, the Office of Homeland Security offers the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) is a one-stop-shop for cyber related information sharing, threat analysis, and incident reporting. NJCCIC is also connected with the New Jersey State Police to support and enhance criminal investigative work.

At the federal level, the FBI Cyber Division not only coordinates cyber-crime investigations, but also provides important real-time threat alerts and other cyber threat awareness information.

All cyber-attacks and breaches should be reported to these state and federal agencies. In addition, for all healthcare provider organizations, other covered entities, and third party business associates that involve patient information, reporting to the U.S. Department of Health & Human Services is required under the HIPAA Privacy Rule.

There are a number of cyber security firms that offer services to monitor suspicious activities inside and outside an organization's firewall. Paying security firms to monitor dark web activities is becoming more common place, as is subscribing to free and paid subscriptions to the latest breach reports and other critical cyber security threat intelligence.

Cyber security is not a challenge that should be left to information technology personnel alone. A strategy that includes employees by making them partners in combating the ever-growing problem is critical. In particular, top leadership can encourage employees to notify IT security personnel about suspicious activity. Creating open communications with employees about sharing suspected intrusions is key to averting potential damages.

Sources:

1. *U.S. Census Bureau, Population Division, State Population Totals and Components of Change: 2010-2018,* *https://www.census.gov/content/census/en/data/tables/time-series/demo/popest/2010s-state-total.html*

2. *Verizon, 2019 Data Breach Investigation Report,* *https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf*

3. *Statista, U.S. Consumers and Cyber Crime - Statistics & Facts,* *https://www.statista.com/topics/2588/us-consumers-and-cyber-crime/*