ENJOY SAFER TECHNOLOGY®

7 VITAL FACTS ABOUT HEALTHCARE BREACHES

www.eset.com

7 vital facts about healthcare breaches

Essential information for protecting your business —and your patients

Large breaches of Personal Health Information (PHI) are regularly disclosed and publicized, and it's evident that this data is highly prized by cybercriminals. According to the FBI, healthcare organizations are a target because they are not as well-protected as more obvious targets such as financial institutions and retailers.[1] A review of recent breach incidents reveals that smaller organizations with limited IT resources are especially prone to compromise.[2] However, organizations of all sizes must adopt a practical approach to understanding and closing the biggest vulnerabilities.

Fact #1: Theft and loss trigger nearly half of breach incidents

Your greatest nemesis isn't criminal hackers. They are laptops and removable drives. Lost or stolen assets figured in 45% of all healthcare data breaches.

Tip: Encrypting PHI is the best preventive measure you can implement. It doesn't prevent loss or theft, but it keeps data that falls into the wrong hands from being read, making it useless. Given the frequency of these incidents, and that encryption removes the federally mandated reporting requirements, there is simply no reason not to encrypt data on any device that might be a target for theft—whether it's in the office or carried home.

Fact #2: Some of the weakest links in your defenses are human, not technological

Overall, 20% of incidents involved misuse of privileges (the "snooping employee" being one example) and another 20% involved various kinds of human errors such as violating policies and misaddressing email.

Tip: Educating employees on safe data handling and computing practices is the best defense here. Encrypting data sent in emails and on devices can help as a secondary measure, but there is no substitute for knowledgeable employees who understand safe practices and the consequences of a breach.

1 FBI Cyber Division, Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain, 8 April 2014
2 Verizon, 2015 Protected Health Information Data Breach Report. We acknowledge this report for the bulk of the data presented in this document.

Fact #3: Smaller practices suffer more data breaches

Of breaches involving healthcare organizations, 55% involved ambulatory practices, mostly smaller physician practices and clinics. Only 40% were at hospitals. (The remainder, approximately 5%, were at skilled nursing facilities and social-assistance organizations.)

Tip: If you assume that your size makes you less vulnerable, shed that false sense of security. The data you have is every bit as valuable to data thieves, and they think you're a better target because they expect your defenses to be weak.

Fact #4: High-volume breaches get the headlines, but stolen credentials remain a threat

Big breaches of medical records stored in databases get the headlines, and rightfully so given the numbers of records exposed. But individual credentials are also a target, and provide an entrée to larger compromises. Keyloggers, phishing schemes and simply guessing insecure passwords are all common avenues.

Tip: First, practice basic security by requiring strong passwords. Install layered security at your endpoints that detects attempts to plant keyloggers, uses multiple methods to stop phishing emails from reaching inboxes, and blocks workers from visiting suspect sites. If you allow access from outside your network, implement two-factor authentication to protect against compromised passwords.

Fact #5: There's gold in your trash

While employee errors are more prevalent at hospitals than smaller ambulatory practices, there's one big exception: employee errors that fall under the category of "improper disposal." It is responsible for 38% of employee error incidents at smaller practices, compared to 22% at hospitals.

Tip: Remind your staff about safe disposal procedures. While many of these incidents involved paper records and films that were left in dumpsters, others were caused by electronic devices with disk drives or flash memory that still contained data. Encryption remains a best practice for any portable device.

Fact #6: A few measures will give you the biggest bang for your security buck

Data breaches often begin with a single event or an attacker exploiting some vulnerability; this triggers a chain of events that eventually leads to data being exposed or compromised. Theft, compromised physical security, abuse of privileges, phishing attacks and data mishandling are the most common initiators.

Tip: If you can put a stop to the most-common initiators, you can make your organization three or four more times complex to attack. Anywhere you can interrupt the chain that leads to data compromise will help protect your PHI. For instance, even if you can't stop all theft, you can implement encryption on your most vulnerable devices so if the item is stolen, it will be inaccessible to thieves.

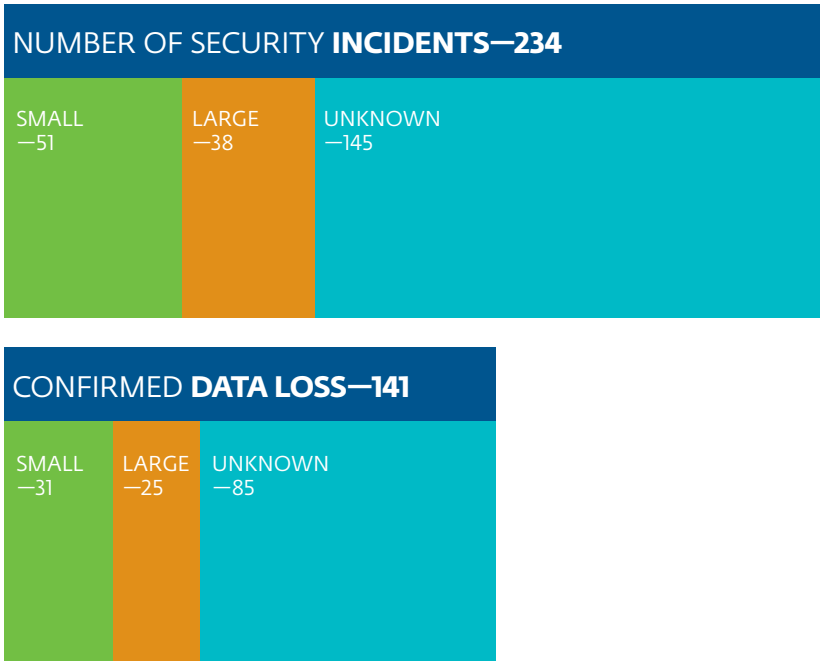
Fact #7: Fear of breaches is compromising medical care

This is the most alarming statistic for healthcare providers. A recent study found that 21% of patients—more than 1 in 5—are withholding information from providers because they fear their personal, confidential information being exposed in a data breach.[3] Given that physicians rely on patients to be forthcoming about their symptoms and to trust the confidentiality of the doctor-patient relationship, this could have a chilling effect on the ability to diagnose and provide the most appropriate medical care.

Tip: Despite the incidence of data breaches, security has been on the back burner as smaller practices struggle to keep up with new mandates. There are, however, ways to implement security that will protect your patients and secure their trust without overburdening your IT staff.

3 Software Advice, HIPAA Breaches: Minimizing Risks and Patient Fears, IndustryView 2015

Healthcare incidents vs breaches



Source: North American Industry Classification System (NAICS)—census.gov/eos/www/naics

Learn more about how to protect your business's important files on hard drives, portable devices and email with *ESET's DESlock+ encryption solutions*. By delivering encryption across all aspects of your enterprise, DESlock+ helps ensure your key asset—your data—is always secure.

About ESET Endpoint Security

ESET Endpoint Security is the easy, effective way to protect healthcare companies of all sizes. By protecting all your devices, including servers, desktops, laptops, tablets and smartphones, it keeps your systems protected against malware and addresses patient privacy as well as HIPAA, HITECH, and PCI compliance. Remotely managed from a central administrative console, this comprehensive protection streamlines security so IT staff can focus on improving the patient experience and quality of care.

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com.

ENJOY SAFER TECHNOLOGY®