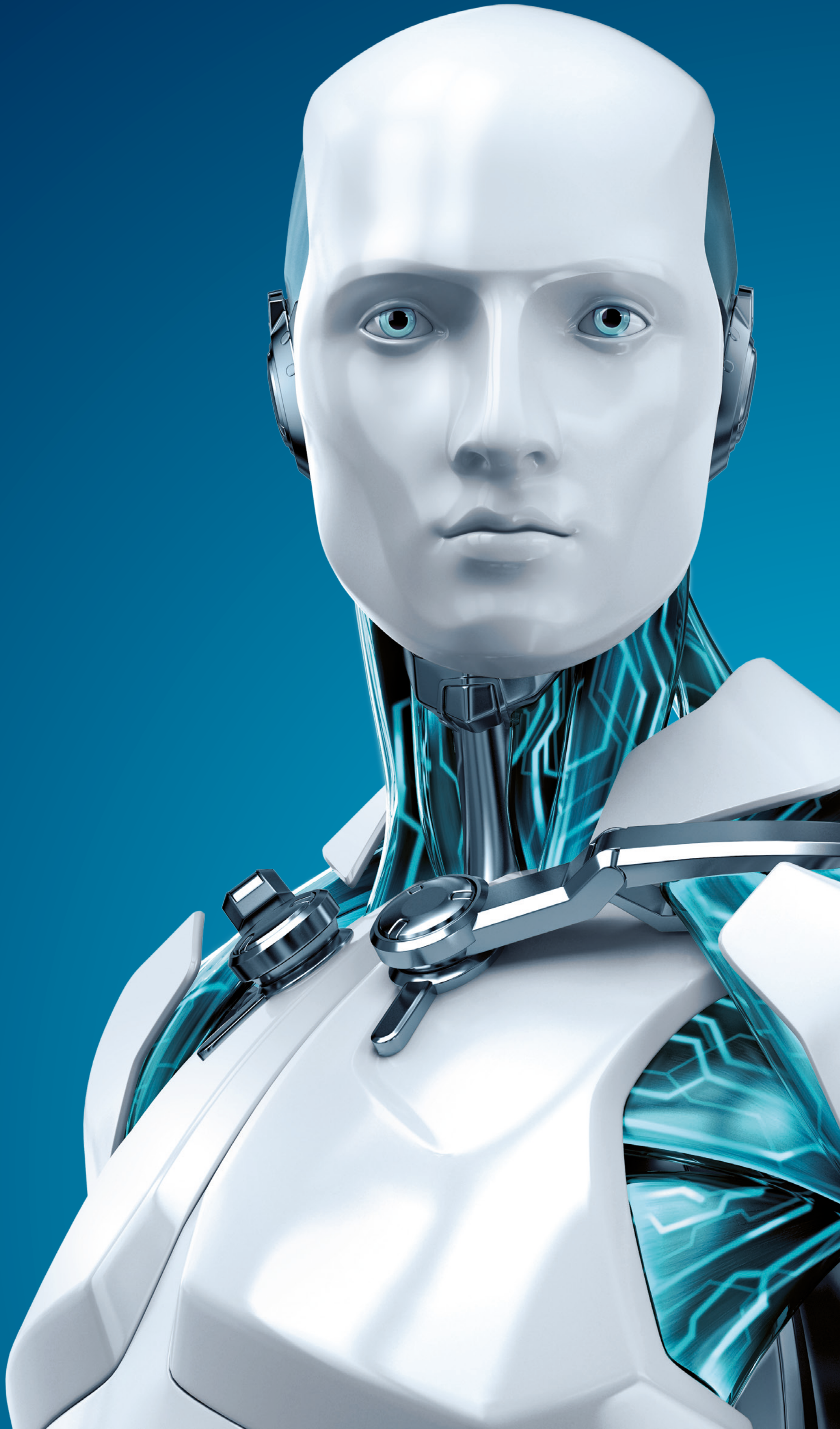
TECH BRIEF

Premera Breach Wake-up Call: Five Security Basics



ESET® ENJOY SAFER TECHNOLOGY™

PREMERA BREACH WAKE-UP CALL: FIVE SECURITY BASICS

Lysa Myers, ESET Security Researcher

In light of the recent Premera breach, the spotlight is more than ever on healthcare businesses and their ability to defend patients' sensitive information. Despite regulations such as HIPAA and HITECH and efforts to comply with them, criminals are still managing to burrow into systems undetected and find exposed data. What else can be done?

In defense of the healthcare industry, part of the problem is the high intrinsic value of the data that systems handle. While compromised credit cards tend to be quickly canceled, stolen medical identities are not as readily detected, since consumers do not check their medical records nearly as often as their bank statements. This gives fraudsters extra time to monetize the information by filing bogus claims, or creating fake IDs to buy medical equipment or drugs that can be resold. Moreover, medical records typically contain extremely personal information, including Social Security numbers for perpetrating sophisticated identity fraud. According to one expert who monitors underground exchanges, stolen medical identities are worth 10 or 20 times more than a credit card number.[1]

This value makes medical compromises the fastest-growing category of data breach. According to the Identity Theft Resource Center, there were 333 medical breaches in 2014, compared with 271 breaches in 2013 — a 23 percent increase year-over-year. Since 2012, healthcare has topped all other industries in the total number of breaches — 43 percent of all breaches during 2014.[2]

So what can healthcare businesses do to reverse this trend? Perhaps we have been so concerned with the intricacies of regulatory compliance that it's time go back and revisit some of the basic principles of online security. At their simplest, the goals are twofold:

1. Decrease the risk of a breach
2. Work to mitigate the damage if an incident does occur

The two work in concert to bolster the defenses. For instance, if an employee's username and password are phished, they are of limited use if the account login requires another authentication factor. A stolen password list is much less useful if it has been salted and hashed. A compromised email server is of much less use if messages containing patient data are encrypted. There is no such thing as perfect security against a sufficiently determined adversary, but it is possible to decrease the value of any one piece of the security puzzle, even if stolen.

[1] "Your medical record is worth more to hackers than your credit card," *Reuters*, http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

[2] "ITRC 2013 Breach List Tops 600 in 2013 (Updated - 2/5/2015)," *ITRC*, http://www.idtheftcenter.org/ITRC-Surveys-Studies/2013-data-breaches.html

Here are five things businesses should be doing to help decrease risk and mitigate damage in case of a breach:

1. Update promptly

Regularly and promptly updating all software is one of the most important things you can do to minimize the vulnerabilities that criminals use to silently get into machines. When you receive a notice from your vendor, go directly to the vendor's website to get the update as soon as possible. Unfortunately, this can be problematic for medical machines, as older devices may still be running a version of Windows XP. This should either motivate businesses to upgrade those machines as soon as possible, or to at least put additional protection in place around the more vulnerable machines.

2. Doubly defend password logins

If you are protecting large amounts of patient data or particularly sensitive information, a password alone is not enough. Consider two-factor authentication. This can be a biometric such as a fingerprint, or a small digital key card, fob, or smartphone app that generates a one-time passcode.

3. Apply the Principle of Least Privilege

The Principle of Least Privilege simply means that no person, machine, or system should have access they do not strictly need. The more limited the rights granted to a user's machine, the less a criminal who seizes control can do with it. For instance: Financial data should be in a different part of the network, and completely cut off from those who do not need to access it. Very few individuals, if any, should have administrator-level access rights on their own machine. Any time you can restrict access without disrupting people's ability to do their jobs, you should.

4. Encrypt everywhere

Encryption is like a lock and key for information. Valuable data should be encrypted whenever it is not directly in use. That means when it is in storage, it should be encrypted. When it is being accessed or sent over the network, it should be through an encrypted connection. Employing encryption from end to end minimizes criminals' ability to get any useful data, even if they do manage to breach your other defenses.

5. Enact redundant defenses

Do not expect one security product to protect you against every possible threat. Install an anti-malware suite on all devices that access your network (do not forget smartphones, Android tablets, Linux servers, and Mac computers as well as Windows machines), and set it to update automatically. In addition to maintaining a hardened, well-configured hardware firewall at the gateway to your network, enable a software firewall on all individual machines.

Medical records are likely to remain a tempting target as long as there is a sufficient return on criminals' investment of time and effort. So while you work to protect your patients' health, you need to take extra care of their data as well. By increasing security, you can decrease the return on investment for criminals, and they may pass by your organization.