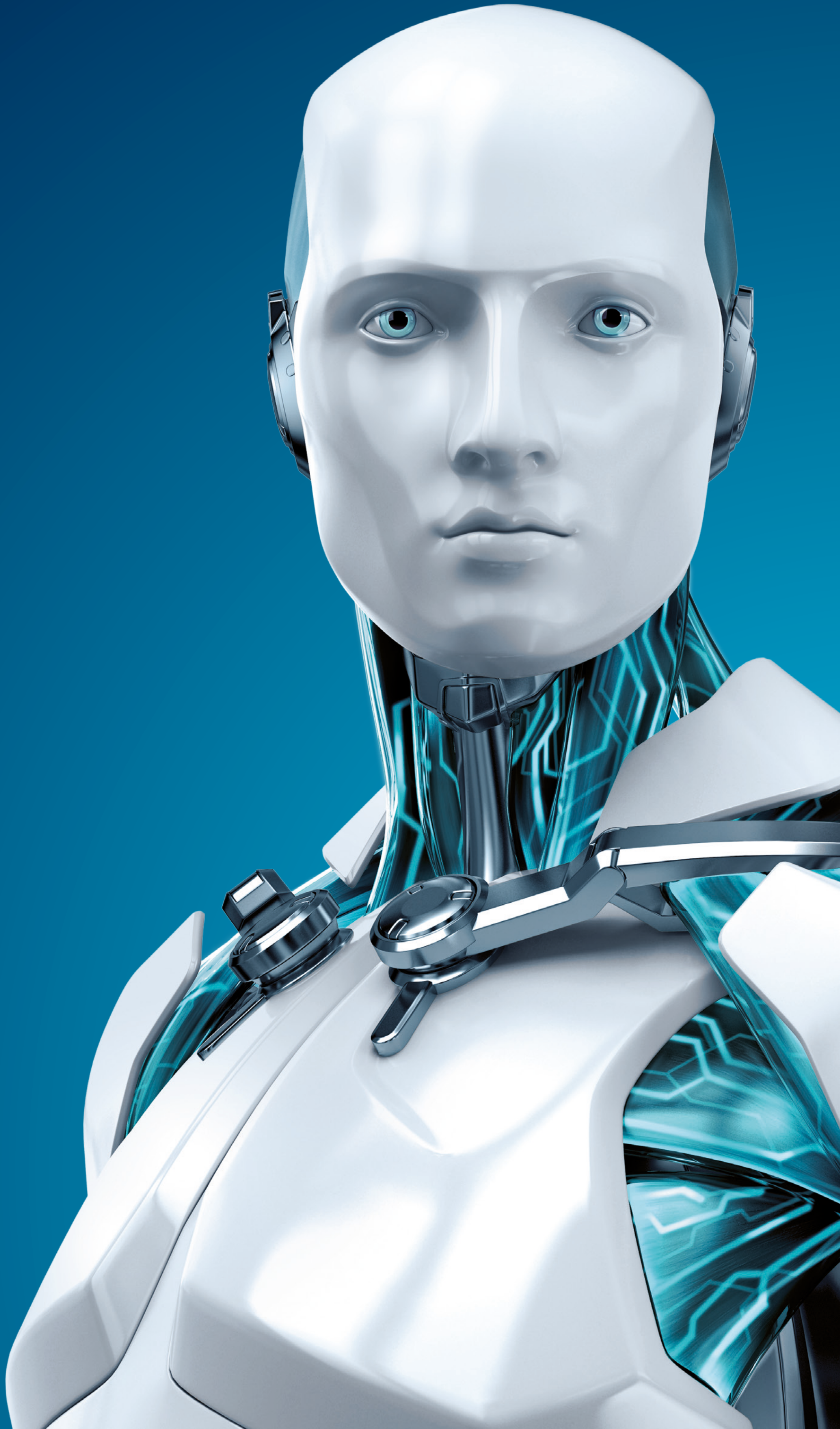
TECH BRIEF

Premera Breach Wake-up Call: Five Basics for Every Business



ENJOY SAFER TECHNOLOGY™

PREMERA BREACH WAKE-UP CALL: FIVE BASICS FOR EVERY BUSINESS

Lysa Myers, ESET Security Researcher

In light of the recent Premera breach, it's a good time for businesses across all industries to take a step back and reconsider their security procedures. Despite regulations and security standards such as HIPAA, PCI-DSS, NIST, and others, and good-faith efforts to comply with them, criminals are still managing to burrow into systems undetected and find exposed data. What else can be done?

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 personal 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.

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. This has proven to be problematic in the healthcare industry, with older medical devices running end-of-life operating systems, but the same applies to embedded systems in equipment used in other industries. Upgrade those machines as soon as possible, or at least put additional protection in place around the more vulnerable machines.

2. Doubly defend password logins

If you are protecting large amounts of personal 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: Personnel data and customer data should be in different parts 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.

How applicable is the Premera episode to organizations outside of healthcare? After all, medical records are an especially tempting target for criminals because of the personal data they contain and the potential for multiple types of fraud. Healthcare tops all other industries in the total number of breaches — 43 percent of all breaches during 2014, according to the Identity Theft Resource Center.[1] Over the same period, the general category of businesses (which includes retailers as well as an astonishing diversity of other companies) accounted for 33 percent of breaches, but 80 percent of the total number of exposed records. Meanwhile, financial institutions accounted for only 6 percent of total breaches and 1 percent of exposed records. This tells us two things: What goes on in healthcare security serves as a bellwether for other industries; and cyberthieves are going after what they perceive as "soft targets," where there is a sufficient return on their investment of time and effort. By increasing security, you can decrease their return on investment, making them more likely to pass by your organization. That is a principle that applies to every organization with assets to protect.

[1] *Data Breach Reports*, Identity Theft Resource Center, December 31, 2014. http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf