Transformation and turnaround in cybersecurity: Healthcare payers and providers

Key findings from The Global State of Information Security® Survey 2016

Some of the biggest healthcare breaches in history were reported over the past year, making protection of digital assets a pressing imperative for healthcare payers and providers. In fact, respondents ranked data-leakage prevention and access management technologies among their top security challenges.

While the healthcare industry has traditionally lagged in the maturity of its cybersecurity programs, some forward-thinking organizations are beginning to take steps to improve their security posture. They are starting to use technologies such as cloud-based cybersecurity, advanced authentication and Big Data analytics.

Organizations are also adopting risk-based cybersecurity frameworks like the NIST Cybersecurity Framework and HITRUST to help guide their overall security practices. As incidents attributed to third-party business partners continue to climb, healthcare organizations are instituting strong policies around required certificates and/or attestations (HITRUST, SOC 2, etc.) for their critical vendors.

Top 5 security challenges

1. Data-leakage prevention
2. Cloud computing
3. Access controls for end users
4. Authentication
5. Identity theft & loss of patient data

Respondents continued to boost security investments in 2015. In fact, healthcare payers and providers said they have increased their information security budgets by 79% over the past two years.

Powerful cybersecurity from the cloud

Cloud computing has emerged as a sophisticated tool for cybersecurity safeguards in recent years as providers offer advanced technologies and processes for data protection and network security. This year, 61% of healthcare payers and providers said they are starting to use cloud-based cybersecurity services.

Some of the cloud-based services that health respondents are starting to embrace include real-time monitoring and analytics and identity and access management. While initial benefits are difficult to measure, respondents said they are beginning to see improvements in monitoring capabilities, threat intelligence and access management.

Advancing authentication to defend data

In an environment in which passwords are considered inadequate, at best, many healthcare payers and providers are turning to advanced authentication to improve access management.

This year, 60% of healthcare providers and payers said they employ multifactor authentication to strengthen access control, while slightly fewer leverage technologies such as hardware and software tokens. Increasingly, organizations also are starting to use biometrics such as fingerprint recognition, as well as smartphone tokens, to strengthen authentication.

The most-cited benefits of advanced authentication tools include enhanced fraud protection, regulatory compliance and security of online transactions. Healthcare payers and providers also said that authentication technologies have helped boost confidence in their security capabilities among customers and business partners.

The intelligence of Big Data

Authentication is key to hardening access controls, but it may not stop skilled adversaries like nation-states from employing complex malware to infiltrate a company's network. As a result, real-time monitoring and analysis is increasingly important to understanding anomalous patterns that could signal a breach in progress. In addition to those who leverage cloud-based monitoring services, 50% of respondents said they use Big Data analytics to improve understanding of external and internal risks, as well as gain visibility into user behavior.

Finally, it has become clear that advanced technologies alone will not stop all cyberattacks. That's why more organizations are purchasing cybersecurity insurance to help mitigate the financial impact of cybercrimes when they do occur. In 2015, 52% of respondents said they have purchased cybersecurity insurance, a double-digit increase over the year before. This finding is significant because it suggests that organizations understand that breaches are all but inevitable, and they are adding safeguards to mitigate the impact of incidents when they do occur.

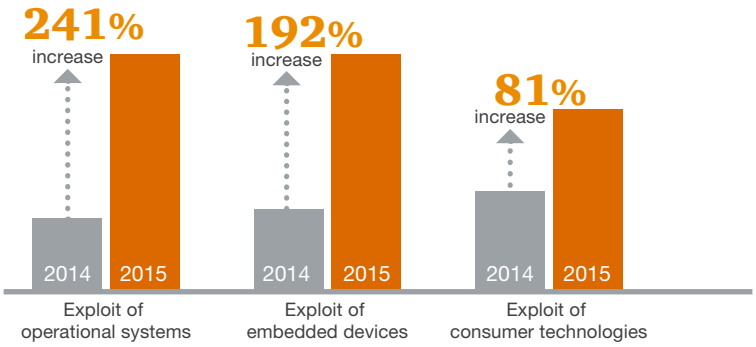
pwc

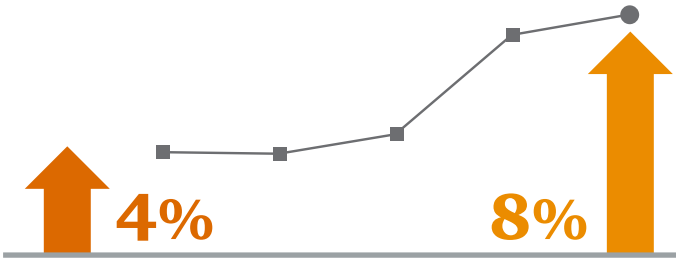
How healthcare payers and providers organizations are responding to rising cyber-risks

56%

Incidents attributed to current third-party business partners jumped **56%** in 2015, an increase that prompted some large US healthcare payers to institute strong policies around required certificates and/or attestations (HITRUST, SOC 2, etc.) for their critical vendors.

Attacks on Internet of Things components like operational systems, embedded devices and consumer technologies skyrocketed.

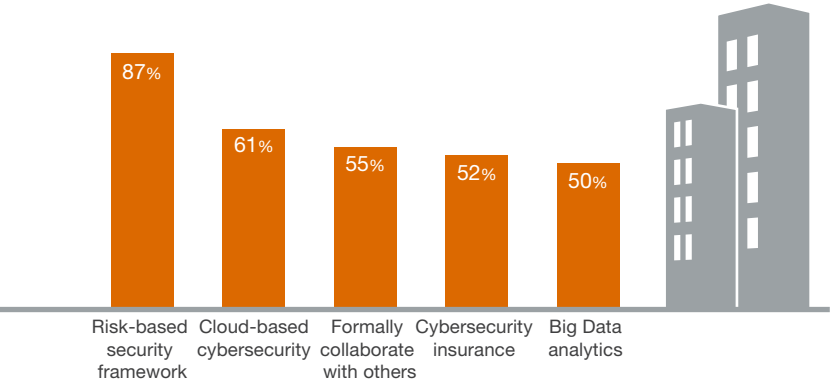




Estimated financial losses as a result of all security incidents inched up **4%** over the year before.

Following last year's huge increase in security spending, respondents boosted their information security budgets by a further **8%** in 2015.

Many organizations are implementing strategic initiatives—such as risk-based frameworks and cloud-enabled cybersecurity—to improve security and reduce risks.



Businesses are investing in core safeguards to better defend their ecosystems against evolving threats.

For a deeper dive into the 2016 Global State Information Security Survey findings go to pwc.com/gsiss or contact:

Mick Coady
Cybersecurity and Privacy
Health Services
(314) 565 1949
mick.coady@pwc.com

Joe Greene
Cybersecurity and Privacy
Health Industries Leader
(612) 481 1938
joe.greene@pwc.com

Timothy Stoner
Cybersecurity and Privacy
Health Services
(317) 418 8740
timothy.stoner@pwc.com

Source: PwC, CSO, CIO, *The Global State of Information Security® Survey 2016*, October 2015