THE PERFECT STORM

WEATHERING CYBER THREATS IN THE HEALTHCARE INDUSTRY

BY DR. BRIAN MCELYEA AND DR. EMILY DARRAJ

In recent years, the healthcare industry has experienced a surge in data breaches, security incidents and criminal attacks.

THE HISTORIC CYBER CLIMATE

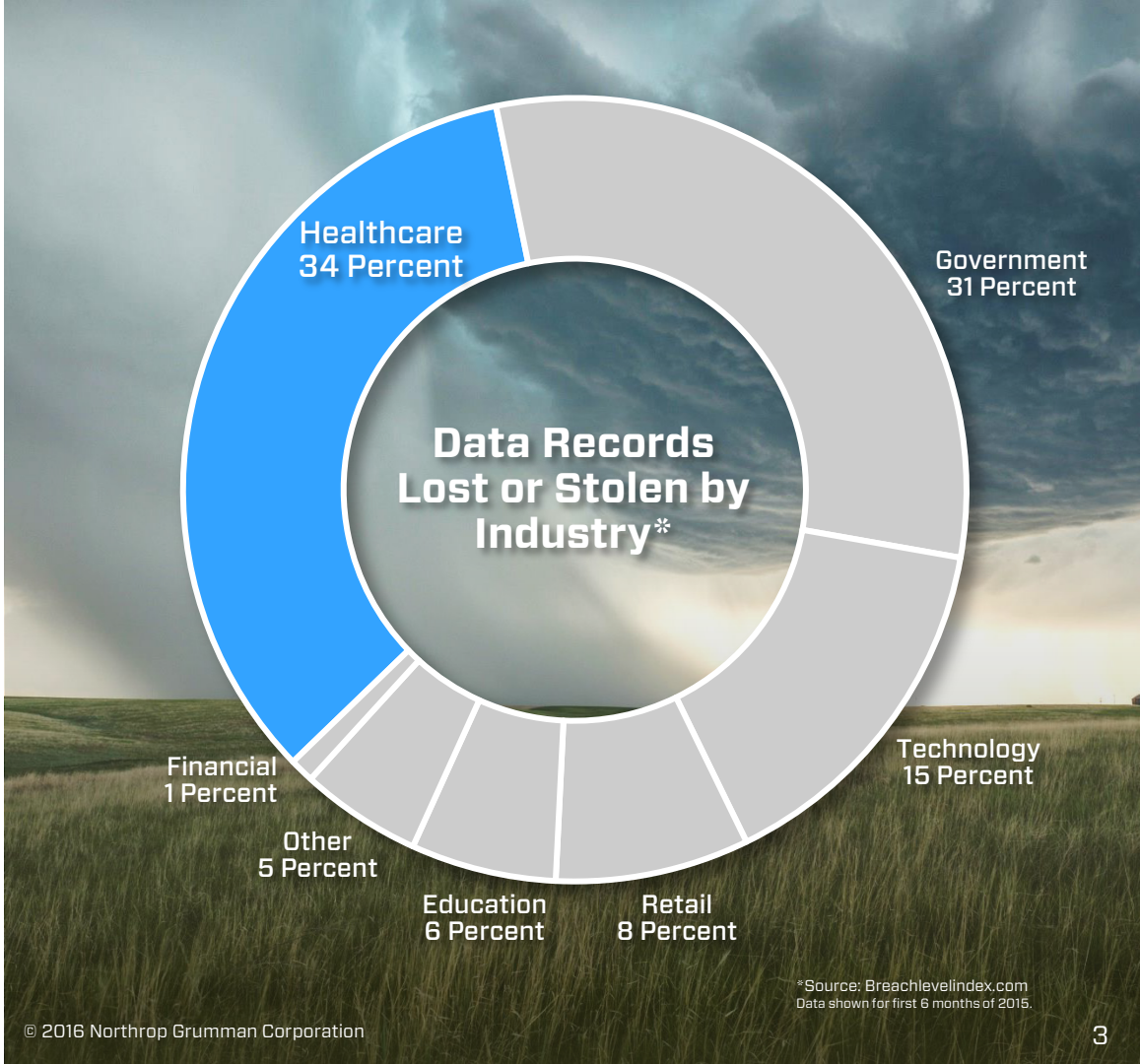
Leading healthcare industry reports show an increase in attacks and in the complexity of those perpetrating the attacks. Sophisticated cyber criminals and state-sponsored hackers understand the increasing vulnerabilities in health IT systems, making it is easier for them to steal individual patient or national health data.

In recent years, the healthcare industry has experienced a surge in data breaches, security incidents and criminal attacks. In 2014, the FBI advised the healthcare sector they were more vulnerable to cyberattacks. Specifically, they warned "the healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of cyber intrusions is likely."

Source: Finkle, J. (2014, Apr. 23). *Exclusive: FBI warns healthcare sector vulnerable to cyber attacks.* Retrieved from Reuters.com.

A STORM IS BREWING

In 2015, the U.S. Department of Health and Human Services breach report documented more than 100 million people were affected by healthcare breaches. In addition to breaches, the combination of vulnerable security strategies with an increasing value of healthcare data on the black market, make the healthcare sector the target of choice for cyber criminals. Based on 2015 predictions, one could surmise these breach trends will continue to climb into 2016, creating the perfect cyber storm.



THE PERFECT STORM

Sophisticated cyber criminals, heightened value of healthcare data on black markets and non-resilient healthcare environments create the right conditions for the perfect cyber storm.

Medjacking is the art of attacking medical devices and their functionality.

CYBER CRIMINALS

The cybercrime waters are rising within healthcare. Attackers continue to develop sophisticated malware bypassing conventional (and often outdated/unpatched) perimeter and security applications. The increasing sophistication of malware targets weaknesses in health information systems. Malware is delivered in elaborate spear phishing campaigns to the end user's computer—where the infiltration starts.

"Medjacking" is the new norm. Medjacking is the art of attacking medical devices and their functionality. These devices range from Internet of Things (IoT) to both embedded and non-embedded medical devices. Attackers exploit health equipment and systems, which incorporate software and microcontroller components in their technology by targeting the insecure software code. This results in a tremendous cost to the healthcare industry. A recent report from Ponemon Institute, found that cyberattacks are costing the U.S. healthcare system $6 billion a year. Previous attack targets in the financial and retail space are being passed up in favor of protected health information (PHI) data.

"...health insurance credentials alone can fetch $20 each; stolen payment cards, by comparison, typically are sold for $1 each."

HEALTHCARE DATA ON THE BLACK MARKETS

The financial incentive for obtaining PHI data continues to remain high. A Price Waterhouse Coopers report stated: "A complete identity-theft kit containing comprehensive health insurance credentials can be worth hundreds of dollars or even $1,000 each on the black market, and health insurance credentials alone can fetch $20 each; stolen payment cards, by comparison, typically are sold for $1 each."

Medical industry networks and data centers as well as medical devices are open to PHI data theft. Cyber criminals can exploit non-resilient healthcare environments to access and exfiltrate PHI data.

As mobile transactions increase, it is reasonable to predict nefarious activity will persist...

NON-RESILIENT HEALTHCARE ENVIRONMENTS

Non-resilient healthcare environments consist of smartphones, medical devices (embedded or non-embedded), health trackers, tablets, computers, wireless connectivity, and personal area networks—all multiple entry points for cybercriminals.

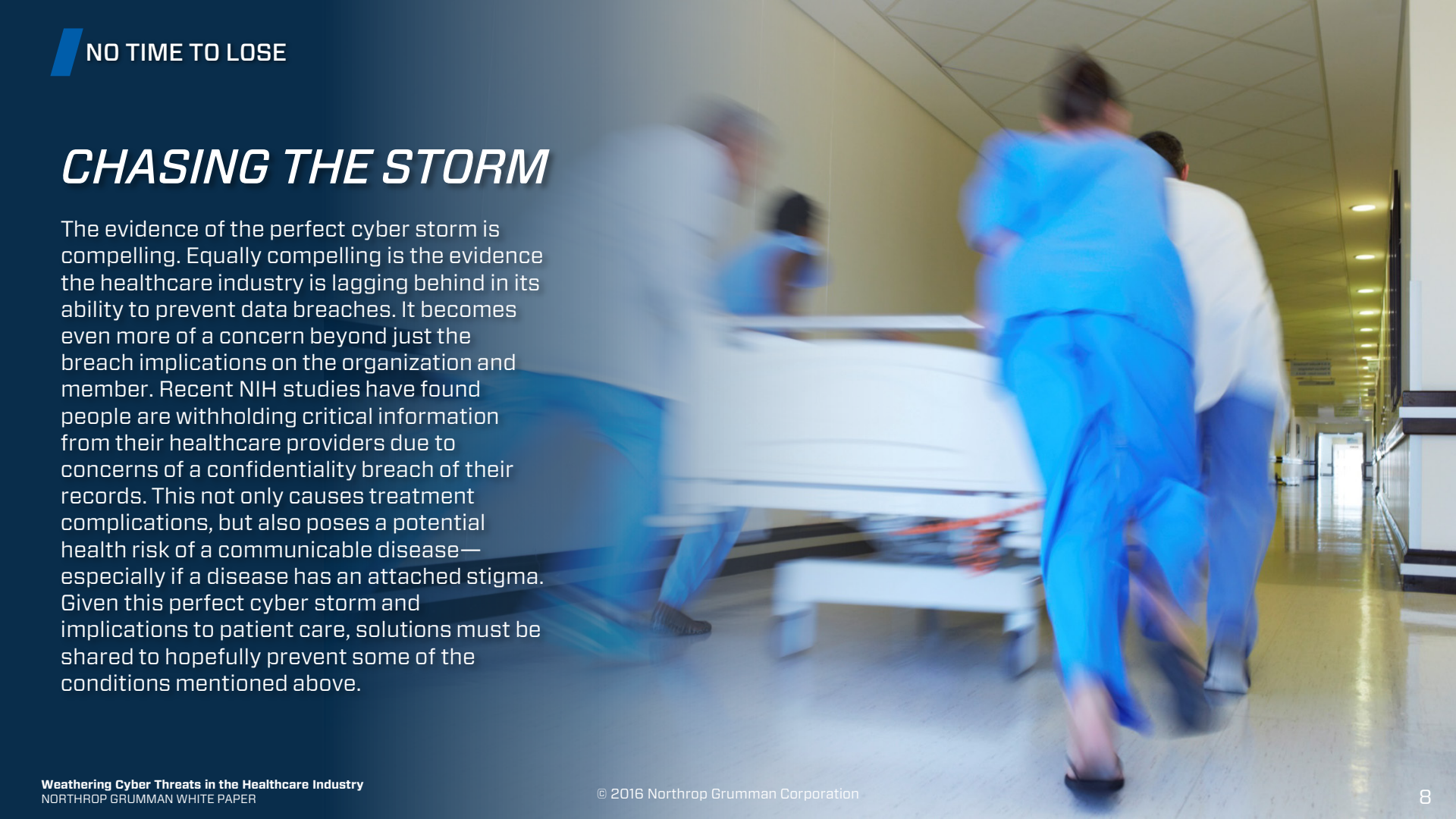
Mobile devices are fertile ground for these groups. As mobile healthcare transactions continue to increase, it is reasonable to predict nefarious activity will persist to intercept these transactions and target healthcare data and systems. Payment systems that allow smartphone transactions are exploitable because the applications in the smartphones have known vulnerabilities.

Industry trends show Insurance and pharmacies are also at high risk. These areas are targeted for the purposes of fraud and exploiting payment systems equally as much as for electronic PHI data.

According to the World Health Organization, the number of people aged 65 years and above is expected to increase from 605 million to 2 billion by 2050. To support this aging population, there has been an explosion in portable health-monitoring devices. In fact, in 2015, 50 percent of the health industry implemented new health-monitoring devices that help comprise the Internet of Things, creating significant additional vulnerabilities for this sector.

CHASING THE STORM

The evidence of the perfect cyber storm is compelling. Equally compelling is the evidence the healthcare industry is lagging behind in its ability to prevent data breaches. It becomes even more of a concern beyond just the breach implications on the organization and member. Recent NIH studies have found people are withholding critical information from their healthcare providers due to concerns of a confidentiality breach of their records. This not only causes treatment complications, but also poses a potential health risk of a communicable disease—especially if a disease has an attached stigma. Given this perfect cyber storm and implications to patient care, solutions must be shared to hopefully prevent some of the conditions mentioned above.



COMBATTING THE STORM

Northrop Grumman continues to leverage significant cyber capabilities to address the privacy and security challenges within the federal healthcare space and defend against cyber criminals and this perfect cyber storm. Integration of cyber resiliency, cyber intelligence and active cyber defense enables layered security, and enhances data protection efforts. This creates defense-in-depth at a level above the industry's current practices and can be foundational in protecting valuable healthcare data and intellectual property.

Everyone loses if there is a breach in any healthcare organization; therefore, we are committed to constantly focusing on how best to protect patient information.

Contact Information

Dr. Brian McElyea
brian.mcelyea@ngc.com

Dr. Emily Darraj
emily.darraj@ngc.com

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN