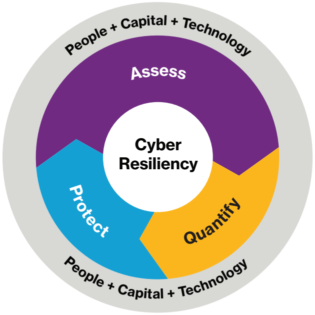


# **Decode** health care.

## Health care organizations are in cyber criminals' crosshairs, but coordinated action can protect you

**By Robert Barberi, Willis Towers Watson**

Cyber exposure for health care organizations has changed significantly over the past couple of years. Prior to the beginning of 2017, mega breaches suffered by large managed care companies accounted for the largest cyber losses. Since then, health care organizations of all types and sizes have seen an increase in frequency of ransomware extortion attacks, distributed denial of services attacks, corporate espionage, privacy violations and network disruptions.

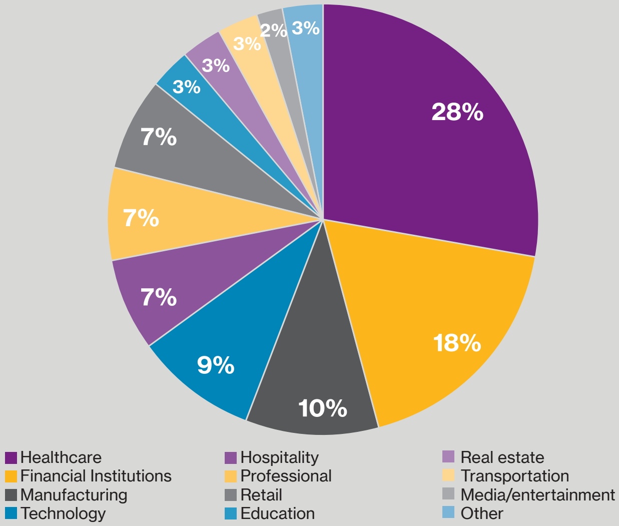
Notably, health care led all industries in claims frequency, representing 28% of total claims reported, compared with 18% for financial institutions, according to Willis Towers Watson's 2017-18 Reported Cyber Claims Index.

High profile network disruptions suffered by a series of hospitals following the Wannacry ransomware outbreak in 2016 illustrate how cyberattacks can impact patient safety. In one large California medical center, patients and staff were forced to relay medical information by telephone, fax machine and shorthand for a week, leading its president and chief executive officer to declare an internal emergency. Subsequently, many health care providers have implemented effective patching and other technology controls to mitigate exposure to ransomware attacks.

But while ransomware attacks have decreased since 2017, hackers are now resorting to new, more creative methods. As a result, health care organizations continue to be prime targets for hackers because covered entities, business associates and customers frequently exchange data, and many of these companies don't have the funds to invest in cybersecurity controls.

**The situation often sparks a healthy debate among senior managers and IT professionals about what best to do about it.**

Claims by industry



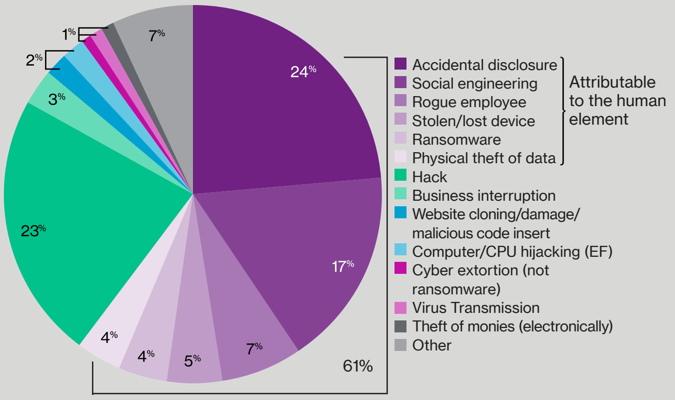
Source: Willis Towers Watson 2017-18 Reported Cyber Claims Index

That's partly because it is often difficult for a health care organization to prioritize investments in its cybersecurity program. Investment options may include improving employee cyber awareness, enhancing technology and compensating controls, and procuring cyber insurance. While practically all cybersecurity professionals will agree that allocating all investment toward technology controls will still leave the organization vulnerable. There is no single clear answer that is universally applicable. Nonetheless, there are certain practical steps that health care organizations can take to mitigate their risk.

## The people problem and how to fix it

According to the Willis Towers Watson 2017-18 Reported Cyber Claims Index, a sizable 61% of the cyber breaches reported were caused by employee negligence or malicious acts, which is comprised of accidental disclosure, social engineering, rogue employees, stolen/lost device, ransomware loss and physical theft of data. Furthermore, our analysis of employee engagement survey data has shown a strong correlation between companies experiencing cyber breaches and certain reported negative aspects of employee experience, including lack of focus on customer centricity, lack of flexibility in decision making, a failure to prioritize respect and teamwork, and lack of training and development that align with pay and performance.

### Type of Loss



Source: Willis Towers Watson 2017-18 Reported Cyber Claims Index

Therefore, taking steps to improve employee engagement should have a direct effect on reducing the likelihood of a significant cyber event. Privacy training (including phishing your own employees) is helpful but shouldn't be treated as the single 'silver bullet' to improve privacy culture. Surveying your workforce to gather insights on cyber-savvy behaviors and perceptions is often a good first step in assessing the people-based vulnerabilities.

## The right analysis can help pinpoint cyber incident costs

Since cyber risk has escalated from an IT to a board-level issue, we see that senior management within health care organizations is more interested than ever in how a material cyber incident could affect the balance sheet. IBM and The Ponemon Institute conduct an annual study of data breach costs, and their 2018 report found that a breach of a single health care record, on average, will cost an organization $408. This number is a good guidepost for smaller organizations that are looking for a general estimate of the tangible (e.g., breach response and legal liability) and intangible (e.g., damage to reputation and loss of goodwill) costs, but the reality is that the individual cost per record will vary depending on the number of records exposed and the factors associated with the data breach (a higher degree of negligence can correlate to higher privacy settlements).

When analyzing network outage losses, the impact assessment often involves further due diligence. It is possible that a cyberattack could result in both a privacy breach and a network outage, and organizations should be prepared to analyze both areas of potential exposure, particularly as the amount of network reliance is often heightened for health care organizations. For example, a patient with urgent care needs will likely try to get admitted to another hospital if a preferred hospital experiences a network outage. Equally important are impacts to productivity. Many organizations can readily demonstrate a contingency plan to operate that isn't electronic, but the costs associated with decreased efficiency are often overlooked.

## Test your incident response policy with live scenarios

Effective incident response can reduce the likelihood of regulatory enforcement and privacy liability settlements. If a health care organization demonstrates that it managed a breach proactively and transparently, this could make it more difficult for regulatory agencies and plaintiffs to correlate alleged damages to negligence. Given that the source of data breaches has expanded to include not only inadvertent employee disclosures of data, but more sophisticated cyberattacks, any incident response simulation should incorporate many different scenarios, including:

1. An escalation protocol
2. An assessment of potential impact to patient safety
3. Assessment of the need for potential notification to the regulator within 72 hours, and effectuation of this notification and potential additional notification to individuals stemming from  requirements of the General Data Protection Regulation (GDPR)

The response to a cyber incident is usually cross-functional and involves internal stakeholders within information security, as well as legal and risk management experts, who may not be in-house. Therefore, participation in an incident response tabletop exercise should include diverse representation.

## Cyberinsurance due diligence

Cyberinsurance policies differ significantly from insurer to insurer. Importantly, given that cyberinsurance is still relatively new, coverages are improving as terms and conditions are refined. Companies may, however, fall foul of the lack of 'standard' (e.g., ISO) forms. Poorly drafted policies can enable insurers to deny coverage for a claim or loss or to delay a payment. Therefore, the scope of coverage is ultimately more important than the limits purchased. Organizations should set aside adequate time to review the policy closely and ask detailed questions of their insurance brokers.

Some key areas of consideration include:

1. **Scope of network business interruption coverage triggers.** Most will include the introduction of malicious code, but this coverage can sometimes be expanded to include system failure, administrative error and beyond. Furthermore, some policies may limit the scope of dependent business interruption coverage; that is, coverage for losses arising out of failure of an outsourced vendor on which the policyholder depends.
2. **Coverage for current GDPR exposures and future California Consumer Privacy Act exposures**. GDPR, which went into effect in May, imposed many significant additional compliance requirements on organizations pertaining to the wrongful collection, use, retention and processing of data. For companies with a significant amount of EU customer data, an affirmative coverage grant for these exposures should be contemplated. The same considerations should be taken into account when it comes to the California Consumer Privacy Act, which will go into effect in 2020.
3. **Coverage for ransomware events.** Cyber extortion losses increased in severity in 2017. Tactics employed by bad actors are constantly evolving. As such, insurance policies must also keep pace. Although many policies include language designed to respond to an extortionist's demand for ransom in order to prevent an attack, often a ransom is demanded after an attack has already occurred. In other words, coverage language needs to contemplate a ransom demand made as a condition to undo the damage already caused, not as a condition to prevent it from happening in the first instance. Further, despite the fact that almost all ransomware attacks demand bitcoins, some forms don't explicitly include cryptocurrencies in the definition of "Ransom". While "monies and/or other consideration of monetary value" is probably sufficient, specifying bitcoins and other forms of cryptocurrency within this coverage is a good rule of thumb.

## Coordinated action is key

While there is no process that will guarantee immunity to a cyberattack, the measures described should help put any health care organization on a path to cyber resiliency. It's important to recognize that cyber risk is difficult to manage because it is implicated in nearly every aspect of an organization - information security, legal, human resources and risk management. Therefore, achieving effective coordination among these stakeholders is critical.

## Contact

**Robert Barberi**
Vice President, Cyber Security & Professional Risk
+1 617 351 7490
robert.barberi@willistowerswatson.com

## About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has over 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

WTW-NA-2018-WTW163861

**willistowerswatson.com**

Willis Towers Watson