

ARTICLE

Skyrocketing cybersecurity insurance costs and rise of attacks: 4 considerations senior healthcare executives should know

<https://www.chartis.com/insights/skyrocketing-cybersecurity-insurance-costs-and-rise-attacks-4-considerations-senior>

It is no surprise that healthcare remains a highly targeted industry by cybersecurity threat actors. Healthcare data is very valuable, many vulnerable legacy systems still exist, and the shared use of data across many organizations creates more avenues to identify weaknesses to exploit. The recent high-profile examples of multiweek-long system outages at several health systems and increases of threats such as ransomware attacks have hospital boards and executives reevaluating how much to invest to effectively manage cybersecurity risks, while balancing other critical decisions related to core operations and other patient care initiatives.

**RANSOMWARE ATTACKS
ACCOUNTED FOR MORE THAN**

50%

of all healthcare data breaches
in 2020.¹

Many healthcare leaders have felt comfortable accepting a certain level of risk with the understanding that they can transfer some risk through the provision of insurance policies that cover cybersecurity incidents. However, with the significant rise of ransomware attacks also came the rise of insurance premiums — which is adding even more pressure to the already difficult job of deciding how much focus and investment in cybersecurity an organization needs.

According to a leading commercial risk solutions company, premiums are expected to increase 20 to 50 percent throughout 2021.² However, considering healthcare is a higher-risk industry, some health systems have already reported increases of 50 to 100 percent for the same or less coverage. Because there is

limited actuarial data on the financial impact of cyberattacks, insurance companies are tightening up cyber insurance policies and revising pricing strategies to cover their own risk.

This reality is leading healthcare executives to evaluate what else they should be doing to balance their acceptable level of risk with a suitable risk transfer strategy that is reasonable and cost effective. This is no easy task. At a high level, we have provided four points for consideration:

1. Face the facts: a cyber incident is “when,” not “if.”

The day will likely come when your organization will experience a cyberattack or major breach: even the most trusted organizations have succumbed to this inevitability. These types of incidents typically create a new urgency with leadership and most often result in an evaluation of what could have been done differently.

In some cases, this heightened awareness leads executives to invest in new technologies that could have significantly minimized the risk. It is important to recognize that insurance companies do not pay for the cost to upgrade or install internal security systems after a cyber event. Therefore, waiting for the pressure to invest in security-mitigating technology after an event has occurred will likely end up costing your organization much more overall, given the total cost a healthcare organization assumes because of an incident.

2. People are your biggest risk.

We have seen that even the most well-funded organizations still experience the impact of a cybersecurity incident as the threat landscape and sophistication of threat actors are advancing at lightening speeds. In many cases, it is internal staff who knowingly or (more often) unknowingly expose the organization to an attack.

The fact that organizations today are averaging 287 days to identify and contain a breach also stresses the need for continued focus on training your staff to lower that timeframe and reduce costs.[3] While continued phishing exercises and ensuring employees feel safe to report their mistakes is always a benefit, equally important is testing your organization’s response and resiliency to an attack. This should be a direct responsibility of healthcare organization leaders; the time and discipline it takes to effectively execute your incident response plan can save time and limit the overall impact of an incident.

3. Insurance should take a back seat to cybersecurity program improvement.

While cyber insurance is very important and can provide many benefits — including access to proven third-party support providers to assist with large-scale cyber incidents — additional focus should be given to further mitigate risks of your current environment. In fact, insurance companies are tightening their

requirements for organizations even to qualify for insurance or to keep premium increases to a reasonable level. The strength of your cybersecurity program may benefit your organization during renewal time. Remember, insurance is “risk transfer,” so there is plenty of work that still needs to be done to mitigate risks down to an acceptable level that decreases the amount of risk transfer an organization needs.

4. Cybersecurity enables an organization’s business objectives.

Gone are the days when cybersecurity should be considered a cost center. If your organization’s strategy involves some level of technology or digital transformation — including moving to the cloud, developing applications, expanding your digital front door, or leveraging new third-party technologies for enhanced service delivery — a renewed focus on cybersecurity can enable your organization to effectively deploy these strategies.

Due to the heightened visibility of cybersecurity risk and the associated costs of attacks impacting the healthcare sector, executive leaders and their boards should be more committed than ever in understanding not only the current threat landscape but also their organization’s security posture, risks, and mitigation strategies.

An organization’s risk posture continually changes with the ever-increasing demand for new technology solutions and data sharing. While cyber insurance is a sound risk transfer approach, refocusing on improving an organization’s cybersecurity maturity will go a long way in not only mitigating risks but also ensuring appropriate cost-benefit of its risk transfer strategy.

Sources

- 1 <https://www.hhs.gov/sites/default/files/2021-hph-cybersecurity-forecast.pdf>
- 2 <https://www.businessinsurance.com/article/20210304/NEWS06/912340248/Cyber-insurance-rates-to-increase-20-50-this-year-Aon>
- 3 <https://www.ibm.com/security/data-breach>

Our services

[STRATEGIC TRANSFORMATION](#)

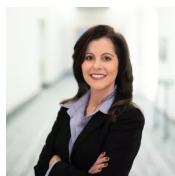
[PERFORMANCE TRANSFORMATION](#)

[DIGITAL & TECHNOLOGY TRANSFORMATION](#)

[CHARTIS CENTERS FOR AI & STRATEGIC INTELLIGENCE](#)

PAYER TRANSFORMATION

STRATEGIC COMMUNICATIONS & CHANGE MANAGEMENT



Angela Rivera

Senior Partner