What's Your Plan?

The Enormous Cost of **Cyberattacks on Healthcare**

JUVARE

More than ever, organizations are having to protect against and prepare for data breaches. Unfortunately, the threat of cybersecurity breaches is only growing as attacks become more sophisticated. No business or organization, large or small, is immune to the threat of cyberattacks. In fact, as former Cisco CEO John Chamber said, "there are two types of companies – those who have been hacked and those who don't yet know that they've been hacked."[1]

Cyber criminals don't discriminate regarding the type of industry or organization they target. Cyberattacks have been carried out on large corporations and small businesses, medical and healthcare, education, government, transportation – you get the picture. The cost and consequences of such an incident on your company, your customers and your brand reputation could be catastrophic if you fail to prepare.

> **"There are two types of companies – those who have been hacked and those who don't yet know that they've been hacked."**
>
> - John Chamber,
> Executive Chairman at Cisco

What are the 5 things you should be doing to prepare, connect and respond in the event of a cyberattack? Certainly, you should have a plan of action, for both IT as well as incident management; but first, how likely is a cyberattack and how will it affect your organization?

The Cost of Cyberattack

In 2017, 54% of companies were hit by cyberattacks that affected data and IT infrastructure.[2]

For example, in 2017, Maersk, the world's largest shipping and supply vessel operator, was hit by a global ransomware attack, which cost the company upwards of $300 million and disrupted operations for two weeks. FedEx was hit by the same ransomware attack, also costing that company an estimated $300 million; and pharmaceuticals company Merck also fell victim, at a cost of nearly $275 million.

The average cost of a malware attack on a company is $2.4 million and the average loss of time is 50 days. But information loss is the most costly element of a cyberattack, making up 43% of the cost.[3]

1. World Economic Forum article, "What does the Internet of Everything mean for security?", by John Chamber, Executive Chairman, Cisco. Jan. 21, 2015. https://www.weforum.org/agenda/2015/01/companies-fighting-cyber-crime/
2. Ponemon Institute, 2017 Cost of Data Breach Study

Protecting Customer Data Means Protecting Brand Reputation

Over and above the cost of downtime and information loss, a cyberattack often has a long-lasting or even permanent effect on a company's reputation. Companies lose credibility and trust, particularly when personal information of customers is compromised. The same goes for hospitals and medical facilities when sensitive patient information is stolen. An IBM/Forbes study found that 46% of organizations say they suffered damage to their reputation and brand value as a result of a cybersecurity breach.[4]

Taking into account costs from customer turnover, customer acquisition, loss of reputation and diminished goodwill, U.S. businesses experienced the highest costs associated with lost business, averaging $4.13 million per company.[4] It's little wonder that "Damage to Reputation/Brand" is the No. 1 risk to businesses, according to a global Aon survey of over 2,000 public and private companies.[5] How you plan, respond or recover from a critical incident can have an enormous effect on your people and property, reputation, and brand.

Bottom Line: Prepare for the Inevitable

There can be little debate that cyberattacks can be costly – not only in monetary terms but also in regard to an organization's brand. These attacks can be debilitating – with enormous loss due to downtime and data loss; or they can be disastrous, with some businesses unable to recover, forcing permanent shut down. While many of the examples here represent some of the most extreme cyberattack instances, all businesses are vulnerable, and the threat is predicted to increase year after year.

Healthcare Organizations at Risk

Cybersecurity continues to plague the healthcare industry as well, with the possibility of even more serious implications. Not only do healthcare organizations face the massive costs associated with cyberattacks, but also the compromise of sensitive patient information could possibly lead to other, more dire consequences including mix-ups in medication or in treating serious conditions which could cause medical emergencies or even death.

The amount of cyberattacks and incidents in the healthcare industry has exploded in the past several years. According to Ponemon, 90% of healthcare organizations have fallen victim to some sort of data breach. However, half of those, according to the study, were caused by criminal attacks and the other half by mistakes by employee or third-party negligence or unintentional errors. Either way, this illustrates how easily data can be compromised. One of the most costly hacks on healthcare in recent years was the ransomware attack on healthcare company Anthem Inc. in 2015, which compromised sensitive personal information of nearly 79 million customers.

> **"The thing that kept me awake at night was cybersecurity. It proceeds from the highest levels of our national interest – through our medical, educational, and personal finance."[6]**
>
> - Admiral James Stavridis, Ret.,
> Former NATO Commander

3. Accenture, 2017 Cost of Cyber Crime Study
4. IBM/Forbes Insights: Fallout: The Reputational Impact of IT Risk
5. Aon, Global Risk Management Survey
6. Gartner Thinkcast interview — Sept. 12, 2017. https://www.gartner.com/en podcasts/thinkcast/blurred-threats-aconversation-with-ex-nato-commander-james stavridis

Bottom Line: Prepare for the Inevitable

There can be little debate that cyberattacks can be costly – not only in monetary terms but also in regard to an organization's brand. These attacks can be debilitating – with enormous loss due to downtime and data loss; or they can be disastrous, with some business unable to recover forcing permanent shutting down. While many of the examples here represent some of the most extreme cyberattack instances, all businesses continue to be vulnerable, and the threat is predicted to increase year after year.

Are You Doing the Right Things to Protect Your People, Property and Brand from a Cybersecurity Breach?

The key to bouncing back from cyberattack is to expect the unexpected. According to data protection researcher Ponemon Institute, the quicker a data breach can be identified and contained, the less it will cost your organization.[7] So, it's essential to have a plan to maintain situational awareness within your organization, to maintain communications and connectedness, and to respond quickly and decisively to a cyber-related crisis.

Take Action: How You Can Minimize the Impact of a Cyberattack

In many ways, a cybersecurity breach is no different from any other critical incident or disaster that could occur that affects the operations and continuity of a business, like a hurricane, flood, earthquake or act of violence. In fact, FEMA includes cyberattacks among other risks such as natural disasters, pandemics, chemical spills and terrorist attacks, in its National Preparedness Goal to "prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."

As with all such incidents, a coordinated, rapid response is the key to minimizing the impact. Response to a cyberattack basically has two components, which should work together simultaneously:

- **Information security tools and procedures to identify malicious activity and dealing with the technical aspects specific to your system. This should include steps for containing the damage and isolating any malware or virus infecting your system and infected devices, as well as analyzing and eradicating the infection.**
- **An Incident Response plan for how to effectively deal with business continuity and the effects of a cyberattack.**

From an Incident Reponse plan standpoint, here are 5 things you should be doing to ensure an effective response to a cyberattack.

7. Poneman Institute, 2018 Cost of Data Breach Study: Impact of Business Continuity Management, p.12.

5 Things You Should Be Doing to Prepare for a Cyberattack

1 Develop a proactive, coordinated organizational response plan and process for taking action and maintaining business continuity in the event of a cybersecurity breach, and for recovery once the threat is eliminated.

2 Implement an incident management platform for situational awareness across your organization with the ability to share real-time incident information, so that everyone involved is aware and up to date on all aspects of an incident. This platform will help your organization make more precise decisions, quickly and more efficiently.

3 Identify all employees, partners and outside vendor services involved in responding to an incident. Make sure everyone on your incident management team knows their individual role and responsibility in responding to an incident. Your incident management platform should be able to notify the appropriate personnel or departments in order to respond as quickly as possible.

4 Communication is essential during and after a cyberattack. Implement a platform that enables quick, easy communication among all internal and external stakeholders during an incident. After the event, be prepared to promptly communicate with customers, partners, stockholders or anyone with your organization who may have been affected. This may include communicating to the media as well as social media. Quick communication about an incident, especially when it has been successfully handled, can help mitigate any negative consequences to your brand.

5 Practice makes perfect. Test your procedures periodically and run periodic training drills simulating actions to be taken during a cyberattack to ensure that your organization is ready to respond. Additionally, it's even better if your incident management platform allows everyday use for monitoring potential threats, so that your team is already adept at using the system and has the experience to spring into action if an emergency occurs.

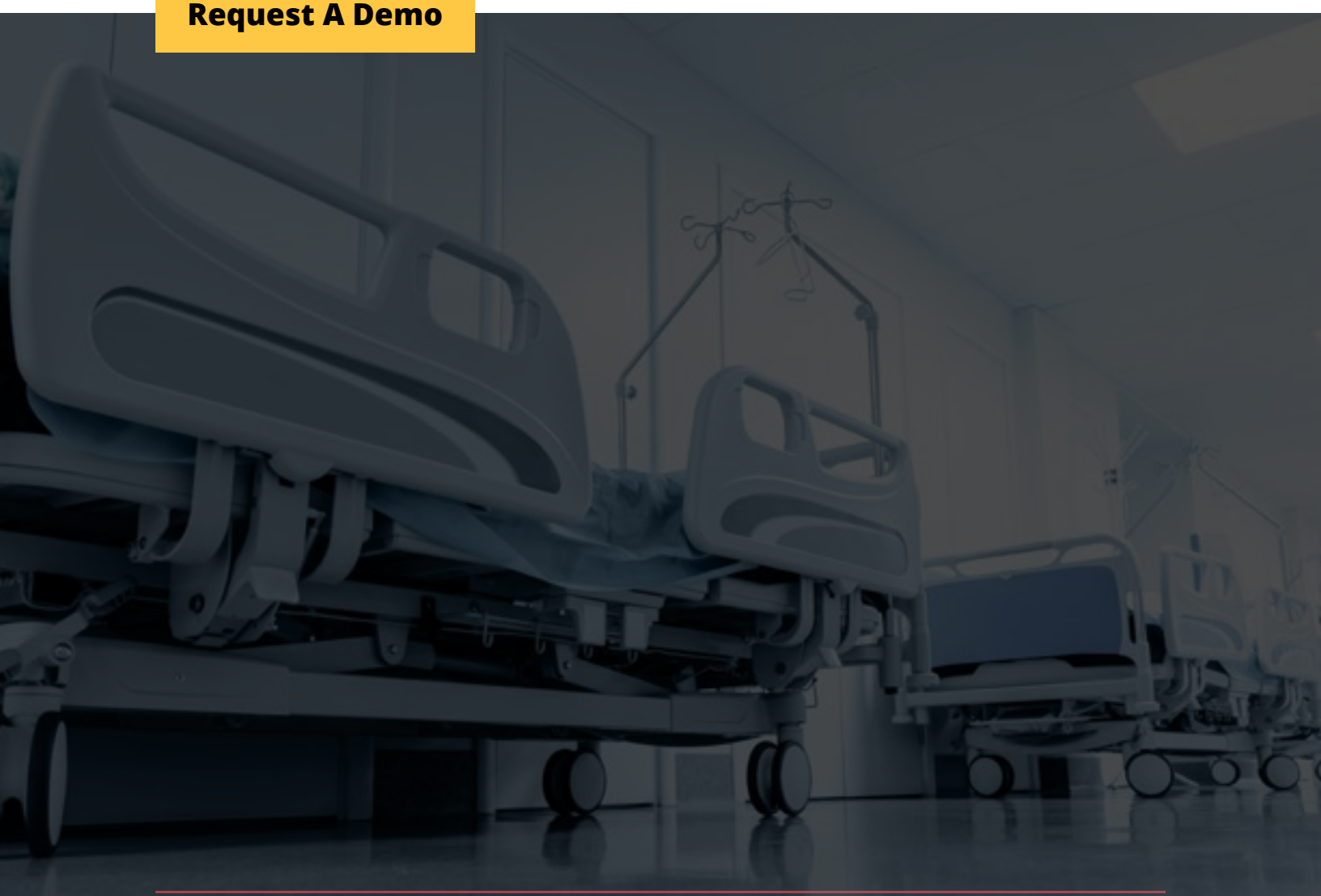
Above all, be proactive. Every minute counts. Organizations must be ready to take immediate action in dealing with any cyberattack.

Juvare Helps Organizations Prepare, Connect, and Respond – Faster

At Juvare, our mission is to strengthen and optimizee information sharing to empower preparedness and response professionals to protect people, property and brands. Juvare is not only the leading provider of emergency management solutions, we are the leader in providing business resilience solutions.

Juvare solutions promote the situational awareness for crisis management and daily operations, connecting your organization's data sources into a common operating picture that's configurable and easy to use. Corporations, healthcare facilities and government agencies alike can use Juvare's solutions to improve communications and information management.

Request A Demo



juvare.com | info@juvare.com | 866.200.0165

JUVARE