The ultimate guide to healthcare cyber security

CYBER DEFENDERS, LLC

FIELD EFFECT / Partners

Table of Contents

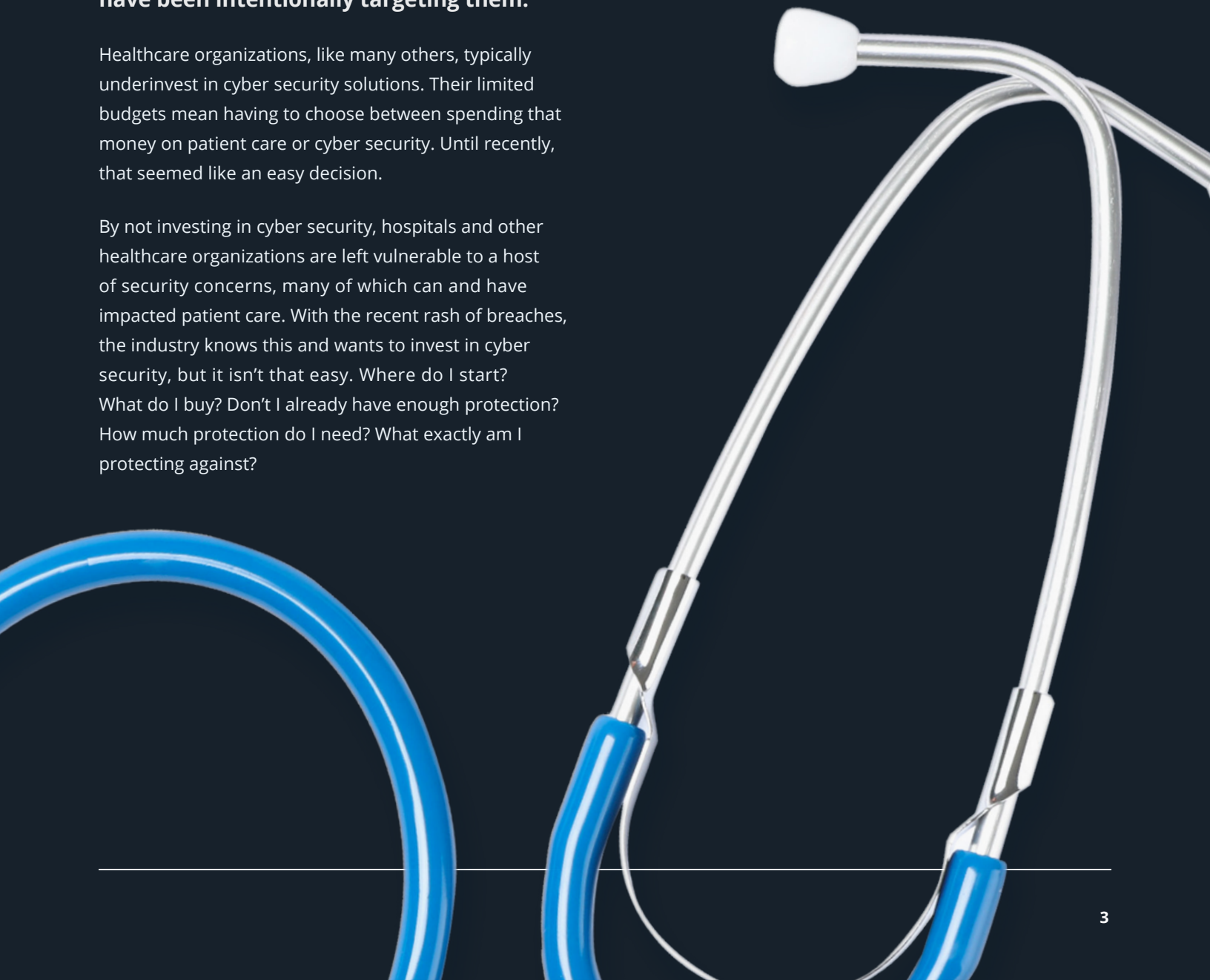
Introduction

We know that today's threat actors are indiscriminate in their attacks targeting small and large businesses alike, but what many of us hoped was that cyber criminals would leave healthcare organizations alone. Not only have they not done that, but they have been intentionally targeting them.

Healthcare organizations, like many others, typically underinvest in cyber security solutions. Their limited budgets mean having to choose between spending that money on patient care or cyber security. Until recently, that seemed like an easy decision.

By not investing in cyber security, hospitals and other healthcare organizations are left vulnerable to a host of security concerns, many of which can and have impacted patient care. With the recent rash of breaches, the industry knows this and wants to invest in cyber security, but it isn't that easy. Where do I start? What do I buy? Don't I already have enough protection? How much protection do I need? What exactly am I protecting against?

These are all valid questions and ones most organizations are grappling with. This white paper will examine the specifics of the problem, explain why healthcare is a target, describe how cyber attacks impact our health structures, and, finally, reveal what can be done to protect you and your business.



Increasing cyber attacks on healthcare institutions

Dr. Josephine Wolff, professor of cyber security policy at Tufts University, puts it plainly: "Cyber security has never been more vitally important for hospitals than it is right now."1

Healthcare institutions are being targeted by cyber attacks at an alarming rate. According to Forgerock's Consumer Identity Breach Report,2 43% of all data breaches in 2020 occurred in the healthcare industry,making it the number one most targeted industry in the US.3

In March 2020, many ransomware operators publicly pledged to leave hospitals and other healthcare facilities alone until the pandemic passed. Some even promised to decrypt compromised data for free.

But this charitable stance didn't last. Before long, cyber criminals began taking advantage of the sudden move to virtual care, overwhelmed facilities, and exhausted front-line staff. Within the first month of the pandemic, the Cyber Threat Intelligence League—a group of volunteer cyber security experts formed to help protect healthcare facilities around the world—identified nearly 400 malicious files circulating.4

In November 2020, the Russian cyber criminal gang known as UNC1878 struck dozens of US hospitals and healthcare organizations, using ransomware to lock their digital systems and control their patient files. That month alone, there were roughly 90 cyber attacks on the healthcare sector every day.

Why are healthcare facilities being targeted by cyber criminals?

There are several reasons why attacks on healthcare institutions are increasing.

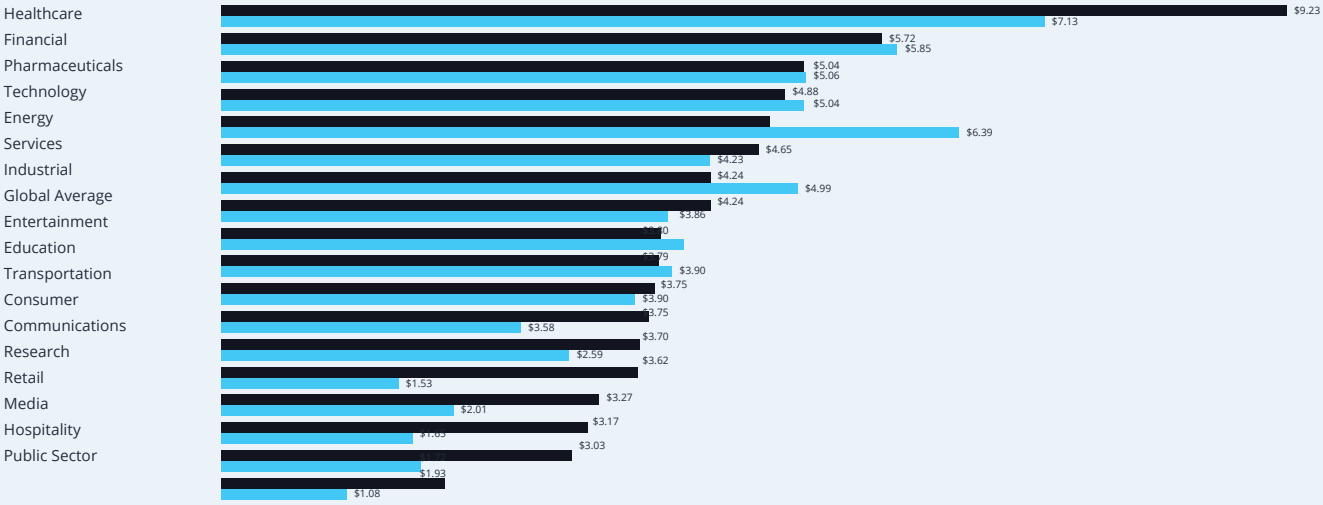
The first is that the data healthcare organizations collect is extremely valuable. Patient data (especially in the US) often contains personal information and financial information—everything from patient addresses and social security numbers to credit card details. Because these sensitive files are crucial to operations and to patients' privacy, hospitals and healthcare organizations will do what it takes to get their data back. Cyber criminals know this.

Even if the institution doesn't pay the ransom, there are other ways cyber criminals can make money. Double extortion is one way, where the attacker demands a ransom from both the institution and the individuals whose data has been breached. And if that doesn't work, they can easily sell the data on the dark web for hundreds of dollars per record—significantly more than financial data sells for.5

Another major reason for the uptick in cyber attacks on healthcare institutions is the pandemic.

Average total cost of data breach by industry6

Measured in US$ millions ■ 2021 ■ 2020



It's no secret that COVID-19 has put enormous strain on healthcare systems around the world. Physicians, clinicians, and other healthcare workers have been pushed to the brink, and cyber criminals are using everything in their arsenal to take advantage of the situation. Often it's done through phishing emails designed to trick exhausted and unsuspecting healthcare workers to click on malicious links that would take them to fake websites impersonating real ones.

The third key reason that the healthcare industry is a target of cyber crime is that it's well known that their security lags behind other industries. As with any money-making venture, criminal or otherwise, if it's successful, it'll be repeated. That's what we're seeing with ransomware. Healthcare organizations are working hard to catch up, but until they do, they will remain prime targets for cyber criminal gangs.

Cyber security challenges facing healthcare organizations

Modern healthcare facilities run on the internet. From electronic health records and the systems on which they run, to e-prescriptions and computerized order entry systems, to the multitude of smart machinery and patient monitoring devices that now fill our hospitals, there is no shortage of entry points for an attack. Innovation breeds opportunity, and in the case of modern healthcare, convenience means exposure.

Continuously Expanding Attack Surface

Working from home. The cloud. BYOD. All of these workplace evolutions—made all the more prevalent thanks to the pandemic—are expanding the networks on which we work. Almost every technology we use connects to the internet in one way or another, which means it could be breached. And the larger and more complex these networks get, the less secure they are

The Abundance of Security Tools

Organizations everywhere are using a growing number of tools to secure their organization, data, and workers — and it's causing problems.7 The sheer volume of technologies and solutions introduces complexity, both in terms of the time needed to manage each individual tool and to integrate them into your environment.

As a result, IT teams and Chief Information Security Officers (CISOs) are facing unprecedented challenges. Organizations with large tech stacks frequently struggle to detect and respond to an attack, compared to those with fewer tools to manage.8 What's more, used in isolation, many of these tools can create silos that make it harder to get a handle on security issues.

Lack of Security Expertise

There simply aren't enough trained cyber security experts out there to manage some of these tools. The New York Times recently reported that, by the end of 2021, there will be 3.5 million unfilled cyber security positions.9

This means that, even if a healthcare organization had the money to beef up its security, chances are they wouldn't be able to find someone to run it. Cyber security talent is being snapped up by the big tech companies and other enterprise organizations who can afford them.

Outdated Software

In March 2020, Wired reported that 83% of medical imaging devices in the United States run on operating systems that are so old, they're no longer eligible for software updates at all, let alone security updates.10

And while the 2017 WannaCry ransomware attack didn't specifically target healthcare, it quickly found its way to them because many British hospitals were running unsupported and unpatched Windows XP and Windows 7 operating systems. By the time the smoke cleared, the National Health Service (NHS), the UK's publicly funded healthcare system, was out over $100 million.

Updating operating systems across an organization takes a significant amount of time and money, so it often falls to the bottom of the priority list. In addition, many healthcare organizations rely on specialized legacy software that simply won't work with newer Windows releases, which means the process of testing new or updated versions of critical software could disrupt patient care.

The impact of cyber attacks on healthcare

According to IBM,the average cost of a data breach is $3.86 million; in the healthcare sector, that number balloons to $7.13 million.11 CPO Magazine reports that, thanks to numbers like these, attacks on healthcare providers became a $13.2 billion industry in 2020.12

It's been estimated that cyber-attacks exposed more than 24 million patient records last year alone.

Legal and non-compliance penalties are also a factor.13 Due to the extensive data privacy regulations surrounding healthcare, when a breach occurs, the fines are steep. If their patient data is ever compromised, Canadian and European organizations governed by PIPEDA and GDPR, respectively, can expect to pay upwards of $100,000 in regulatory fines.

But the costs to hospitals and other health facilities isn't just financial. In the United States, where healthcare and medical services are largely privatized, any amount of brand damage can be devastating, resulting in a client trust deficit that can take years to climb out from.

The UHS Attack

With more than 90,000 employees, United Health Services is among the largest healthcare companies in the world. It operates 400 hospitals and medical facilities in its network, serves more than three million patients a year, and has been ranked in the Fortune 500 since 2003. That's why the attack made such headlines.

On September 28, 2020, UHS announced that its network had gone offline the previous day, with computer and phone systems suddenly being locked. Spokespeople blamed an "IT security issue."

That issue turned out to be a ransomware attack.

Electronic health records at all 400 facilities were affected, and services were disrupted for weeks.

All told, the cyber attack ended up costing UHS $67 million.

How to choose the right solution for your organization

When assessing any solution, there are four factors to consider:

The question on every health professional's lips should be "How can we best secure our environment against cyber-attacks and prevent the catastrophic damage that so many other outfits have had to endure?"

Long question, perhaps, but the answer is simple: threat detection and response.

Detection and response solutions can identify threats that have snuck past your defenses and respond to them. Detection relies on visibility and the combination of data from multiple planes of threat. But with a single solution that scans your entire network and collects the relevant data in a known format and in a single data store makes it easier to do complex analyses, derive insights, and identify threats.

Trying to find the right cyber security solution to protect your organization can feel like trying to find a needle in a haystack. Not all solutions are created equal, which makes finding one that will meet your organization's needs all the more challenging.

Solutions must keep pace with the rapid changes in the cyber security landscape. Any chosen software should provide functionality and capabilities to identify potential risks and active threats across your IT infrastructure, provide actionable alerting, and help you prioritize and remediate any issues.

Scalability: How will this technology adapt to changing needs?

Businesses are always changing and growing. Each new user creates a need for additional technology, which in turn expands the threat surface. Customers introduce additional requirements and concerns.

Look for a solution that deliver a range of capabilities, backed by a vendor that's committed to continual improvement and developing and releasing new features for a strong defence.

Holistic approach: How comprehensive is the solution's approach to security?

While the techniques behind each cyber threat may overlap with each other, they're not all targeting the same component, and their end goals may differ wildly. If a solution focuses exclusively on one aspect of the threat surface at the expense of others, this may require deploying multiple solutions to solve each new issue.

Effective cyber security requires an end-to-end approach to monitoring, detecting, and responding to threats and risks across the entire IT environment. This holistic approach to security should protect endpoints, cloud services, and IT networks, 24/7, 365 days a year.

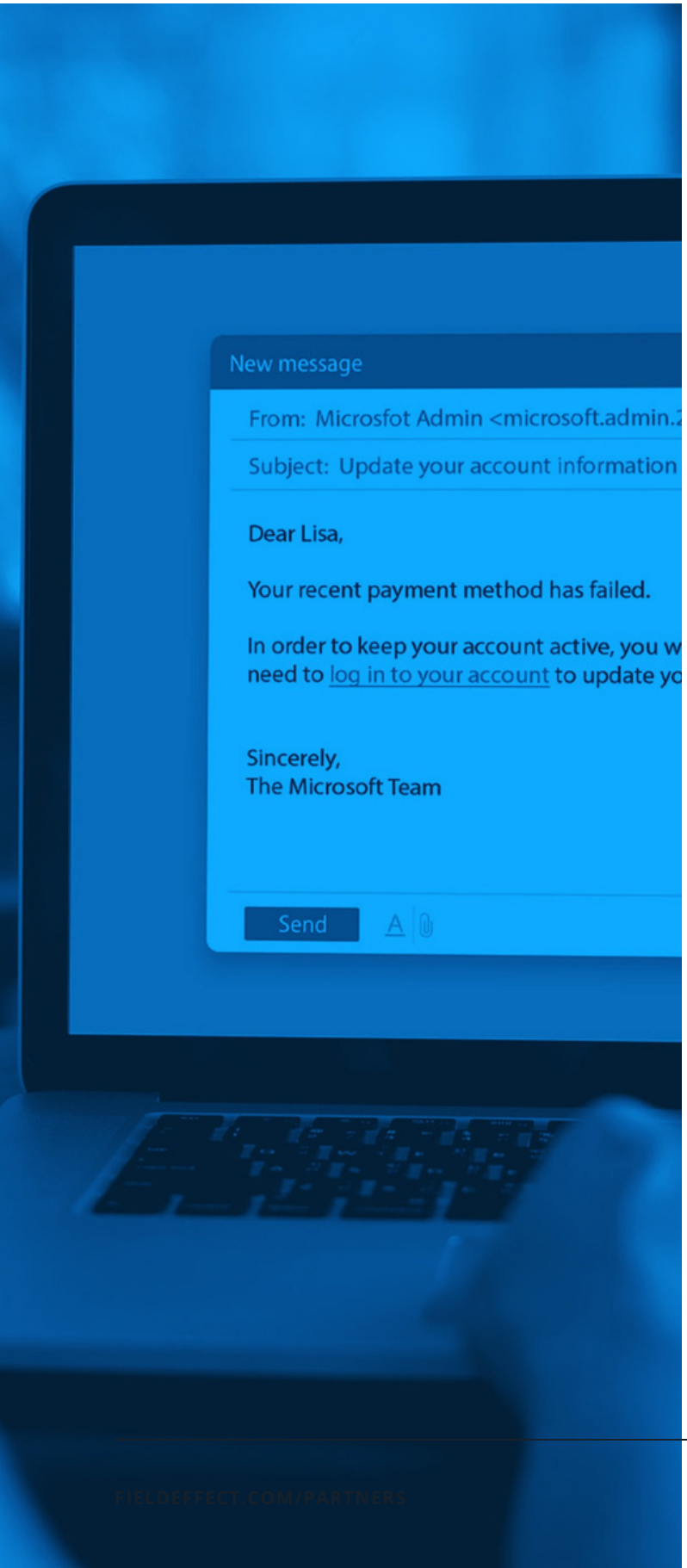
Unfortunately, some vendors only deliver this coverage through modular add-ons, requiring additional IT investment to implement effective defences, as well as more time to integrate, manage, and maintain. Solutions that take this holistic approach can deliver effective security coverage without the sticker shock at renewal time.

Expertise: How experienced is the security team backing the solution?

At its core, cyber security is about knowing how threats work, how to spot them, and how to respond to them. Cyber security automation can provide some relief, but human analysis is still necessary to interpret

the data gathered by any solution. Because hiring an in-house team is costly and time-consuming — not to mention more and more difficult due to the scarcity of available talent, many businesses choose to outsource some or all of their cyber security defence, hiring experts and relying on managed service providers.

Ensuring solution providers can back up their technology with the necessary expertise is vital. Take time to check credentials, review client testimonials, request references, and ask about the product roadmap — look for a team that brings deep experience in cyber security along with software development and management.



Time: Will the solution automate common, time consuming security tasks?

Cyber security can be time-consuming and challenging, and attackers know it. That's why techniques like business email compromise (BEC) continue to be effective — they rely on just how busy and overworked IT teams are. CISOs and IT teams are stretched thin from the constant demands and information overload of cyber security. Burnout is common, with teams struggling to handle security tasks on top of daily IT needs.

When it comes to threat monitoring, detection, and response, look for effective and efficient solutions that monitor the vast amounts of data activity from IT networks, endpoints, and cloud services. From there, narrow it down to tools backed by a team of cyber experts that not only thoroughly analyzes this data, but provides clear, actionable information to help prioritize and triage response and remediation. This functionality reduces the time required to investigate false positives and focus on the threats that matter.

Conclusion

Finding the right solution can sometimes feel like a daunting task, especially as you deal with day-to-day security challenges and other critical IT priorities, but we hope this white paper has given you the valuable insight you need to make the right choice.

If there's one thing you take away from what you've read, we hope it's that you understand not all solutions are created equal. Finding one that will grow with you while providing comprehensive, end-to-end defence has never been more urgent.

Cyber threats are always changing. You deserve protection that can keep pace. Taking a proactive approach to defending and securing your operations against new and emerging risks can help prevent cyber attacks.

And, remember, you're not alone. It's our mission to help protect small- and mid-sized businesses. If you have any questions, or need any help with your cyber security, get in touch with our team.

We've got your back.

Sources

1 https://www.nytimes.com/2020/10/17/opinion/hospital-internet-security-ransomware.html

2 https://www.forgerock.com/resources/2020-consumer-identity-breach-report?utm_campaign=Amer-All-IdentityCloud&utm_source=adwords&utm_medium=search-paid&adgroupid=124367955114&gclid=CjwKCAjwtdeFBhBAEiwAKOly5z2IZ5zOz12_XvGfaA6z0oIQQfBCWKHC60Mj4tCwdHWzZL3YaHCY0R0C5eIQAvD_BwE 1

3 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/

4 https://cti-league.com/

5 https://pubmed.ncbi.nlm.nih.gov/30488291/

6 https://www.statista.com/statistics/387861/cost-data-breach-industry/

7 https://www.esg-global.com/blog/security-point-tools-problems

8 https://newsroom.ibm.com/2020-06-30-IBM-Study-Security-Response-Planning-on-the-Rise-But-Containing-Attacks-Remains-an-Issue

9 https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html

10 https://www.wired.com/story/most-medical-imaging-devices-run-outdated-operating-systems/

11 https://www.ibm.com/security/data-breach

12 https://www.cpomagazine.com/cyber-security/healthcare-cyber-attacks-rise-by-55-over-26-million-in-the-u-s-impacted/

13 https://fieldeffect.com/blog/real-cost-data-breach-2021/

About Cyber Defenders LLC

Cyber Defenders, LLC is a Service Disable Veteran and Minority owned Managed Security Service Provider and software development firm. We, along with our partners, provide a hands free managed detection and response solution. We protect your endpoints, networks and cloud services – all from one platform. From easy-to-use 24/7 monitoring with cyber experts at your side to deep threat hunting, DNS security, incident response, IDS/IPS, and more — we have you covered.

Contact our team today

Email
r_wyche@cyberdefendersllc.com

Phone Number
888-314-9444

Website
https://cyberdefendersllc.com