Threat report

How are different industries battling cybercrime?

A report by
Siteimprove Web Security

Siteimprove

Contents

Executive summary	3
About this report	4
Education	6
Healthcare	10
Financial services	14
Government	18
Retail	22
Manufacturing	26
Take control of your web security with Siteimprove Web Security	30

Executive summary

Web security is quickly emerging as a key competitive differentiator in today's marketplace. In fact, **73% of leading organizations now view strong cybersecurity** as a key contributor to business success. Organizations of all shapes and sizes are beginning to understand that if they don't adequately protect their websites, they risk consequences from regulators and backlash from security-minded consumers.

"Cybercrime is the greatest threat to every company in the world."

Ginni Rometty, Chairman, IBM

Today, many consumers perceive strong web security as a non-negotiable part of dealing with an organization. In fact, a PWC study found that **85% of consumers won't do business with a company** if they have concerns about its security practices. The expectation is that businesses must proactively manage cybersecurity and privacy risks – or risk losing their customers' trust.

Protecting your website has always been important, but since the start of the coronavirus pandemic, web security has become business critical. Security experts have witnessed an **800% surge in cybersecurity attacks**, targeting everything from small businesses and local governments, to high-profile attacks on Honda, Canon, and Twitter.

It's no understatement to say the stakes are high when it comes to web security. The negative consequences of a security breach aren't just limited to an immediate financial cost, but also include loss of brand equity, legal action, damaged reputation, adverse shareholder impact, search engine blacklisting, stretched resources, increased customer turnover, and lowered employee productivity.

About this report

This report analyzes the web security standing of 8,345 website domains across North America, Europe, and Asia. The domains have been analyzed based on industry and are broken down into education, financial services, government, healthcare, manufacturing, and retail. The sites have been scored using Siteimprove Web Security's scoring system, which includes three categories and an overall weighted average (measured on a scale of 0 to 100).

Overall score: This is a weighted average score of the other three scores and provides a high-level overview of a domain's web security standing.

Web application score: This category scores a website's on-page content, cookies, encryption, and certificates used to secure content. This score assesses how well a website's on-page content meets best practices. Examples of issues that can affect this score include a domain that does not enforce HTTPS-encryption or expired certificates.

Network score: This category scores malware activity, attacks on the network over time, Sender Policy Framework (SPF) records, and phishing attempts.

Server score: This category scores known vulnerable systems and configurations found in the website's hosting, database, or server setups. Examples of issues that affect this score include high severity CMS vulnerabilities, SSH protocols vulnerabilities, and End-of-Life Products warnings.

How scores are gathered

Siteimprove Web Security combines data from third parties that have partnered with Siteimprove, as well as additional Siteimprove insights and findings that include:

- Scans (active)
- Crawls (active)
- Sensors and data feeds (passive)
- Honeypots
- Sinkholes
- Identifying ports and IP-addresses (active)

This lets us provide a thorough analysis of a domain's weaknesses and vulnerabilities.

Score overview

For reference, here are the scores for each industry.

Industry	Average score	Web application score	Network score	Server score
Education	68	59	90	54
Finance	78	61	96	78
Government	80	68	96	77
Healthcare	80	66	92	80
Manufacturing	73	56	90	72
Retail	74	61	89	73
Other	78	65	92	78
Average	**78**	**64**	**93**	**76**

Education

Education, from K-12 to colleges and universities, has changed completely through the coronavirus pandemic. Many students and families will learn remotely for months or longer, which has created unique opportunities and a host of challenges—not least among them: cybersecurity.

Cybercrime increased overall during the pandemic. A report from INTERPOL has said that **the rate of cyberattacks during coronavirus has been "alarming."** Educational institutions and systems, and higher education in particular, have been hit hard. **CyberShark even says**, "Security breaches happen with frightening regularity in higher education."

While all educational systems and organizations face heightened risk, higher education institutions face more risks than K-12, as they handle both personally identifiable information, as well as valuable research data.

The challenges education organizations face when it comes to web security often fall into three main categories.

Main challenges for education organizations

1. **Large, complex systems**
2. **Insecure devices**
3. **Poor training and large populations**

1 Large, complex systems

Higher education institutions often run on old, legacy systems—which are a far cry from the cutting edge technology and methods hackers use. Colleges and universities not only have legacy systems to contend with, but those systems are usually large and complex.

"Cyber-attacks on universities occur frequently not because the systems lack protections, but because they are so large and complex that implementing those protections becomes difficult,"

writes Don Carfagno for CyberShark.

Departments and schools often have their own IT staff or don't communicate with a centralized IT department, making it impossible to understand what kind of sensitive data they have or need protected. This creates a patchwork system that is incredibly difficult to protect.

2 Insecure devices

Perhaps one of the easiest to understand threats to educational organizations is the fact that students, faculty, staff, and volunteers all access school systems with personal devices. Those personal devices might run on outdated software or be "jailbroken," both of which pose security risks.

It's impossible for IT to ensure software is updated on all devices or that all devices accessing the network are secure, making the system vulnerable to hackers.

3 Poor training and large populations

Another significant web security challenge for the education sector is the sheer size of the student body and staff. **Large student bodies make it difficult to ensure proper web security training**—including creating strong passwords, recognizing phishing attempts, and ensuring software is updated.

And this poor training has resulted in behavior that can cause security risks: "30% of users in the education industry have fallen for phishing scams posing as corporate communications, double the rate of the general population, in the last year," **according to Toptal**.

K–12

Higher ed isn't the only segment of the education sector that faces web security risks. **According to Forbes**, 74% of K-12 organizations do not use encryption. Forbes also says that 93% of K-12 organizations rely on native client/patch management tools that have a 56% failure rate.

Education scores lowest of all industries ranked by Siteimprove Web Security

We analyzed 2,410 higher education and K-12 domains across Europe, Asia, and North America. The average Siteimprove Web Security score for education is the lowest of all measured industries at **68 out of 100**.

If you look at the category level scores, there's a huge variation in how education performs. On average, education domains only have a server score of 54 and a web application score of 59—however, their network score is 90.

That indicates that educational institutions are safer from malware activity and phishing attempts. However, they have weak hosting, server setups, high CMS vulnerabilities, weak encryption, expired certificates, and vulnerable on-page content.

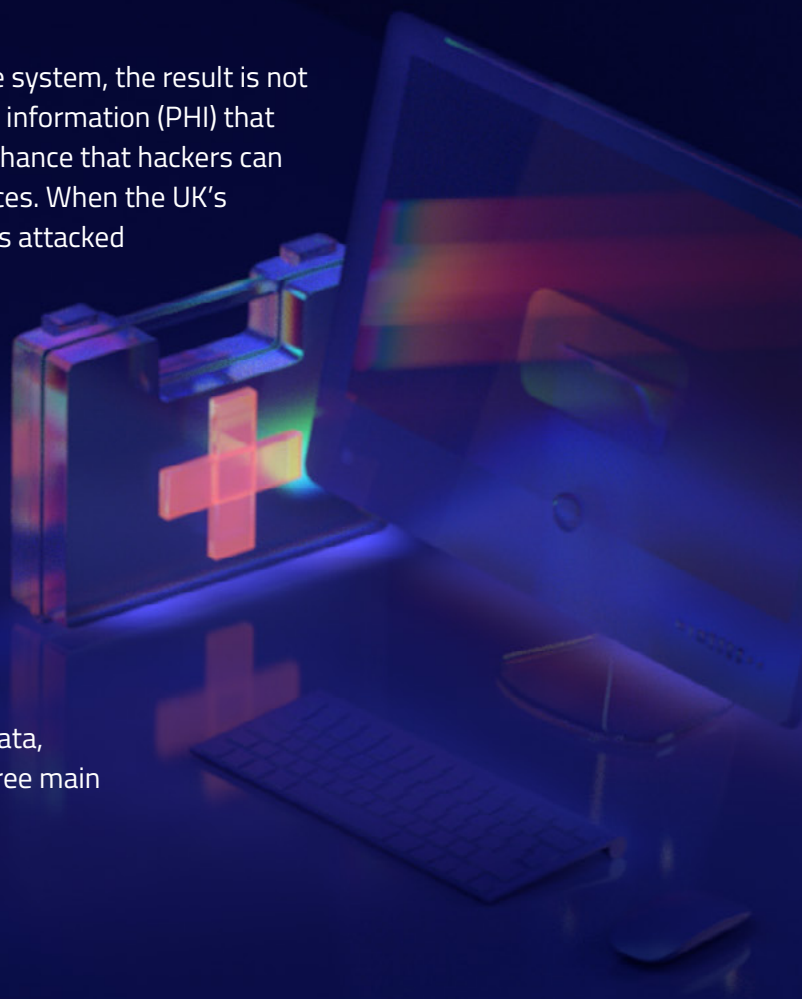
All in all, the state of the education sector's web security is highly concerning—especially when thinking about potential data breaches.

Web Security score

Healthcare

Healthcare has been hard hit in recent years by hackers with financial motives. But unfortunately, as Nicole Wetsman writes for The Verge,

"Experts say that healthcare lags far behind other industries, like the financial sector, in the way it protects its information technology infrastructure. And unlike finance, a healthcare failure can end with injury or even death."



When hackers attack a healthcare system, the result is not "only" leaked personal healthcare information (PHI) that creates risk—there's a very real chance that hackers can freeze hospital systems and devices. When the UK's National Health Service (NHS) was attacked in 2017, there were 20,000 appointments cancelled and 1,200 pieces of diagnostic equipment affected.

On top of that, there have been a number of incidences where **hacked hospitals had to revert to paper charts to continue providing care**.

When it comes to hospitals and care services protecting patient data, they typically come up against three main challenges.

Main challenges for healthcare

1. Internal threats
2. Device security
3. Ransomware

1 Internal threats

According to the Verizon 2019 Data Breach Investigations Report, a whopping **59% of healthcare data breaches are caused by internal actors, making it the only sector with more internal bad actors than external.**

"The role of negligent insiders in critical healthcare infrastructure is only becoming more apparent," **write the authors of one study on cyber threats in healthcare**. "The need for improved technology needs to be balanced against the need for user education and policy centered around the user that exposes critical healthcare infrastructure," they say.

Generally, **medical staff are very poorly trained on cybersecurity, and yet work with extremely sensitive data and connected devices.** That makes accidental insider threats, such as phishing, much more likely.

Hospitals should audit and report on who has access to which data and systems, as well as implement data backups and closely monitor PHI from being sent via email or web upload.

2 Device security

Medical devices are increasingly smart devices, which allows healthcare professionals to treat patients more effectively and conveniently. However, smart devices naturally come with an increased risk of cyberthreats, as the devices can be hacked. In 2017, for example, **almost half a million pacemakers needed a firmware update to avoid getting hacked**.

In the US, the FDA is working with manufactures, providers, and patients to create **a framework for talking to patients about cyber vulnerabilities** in their care and devices.

The FDA knows this is a very serious problem for patients and the healthcare system, **commenting that**,

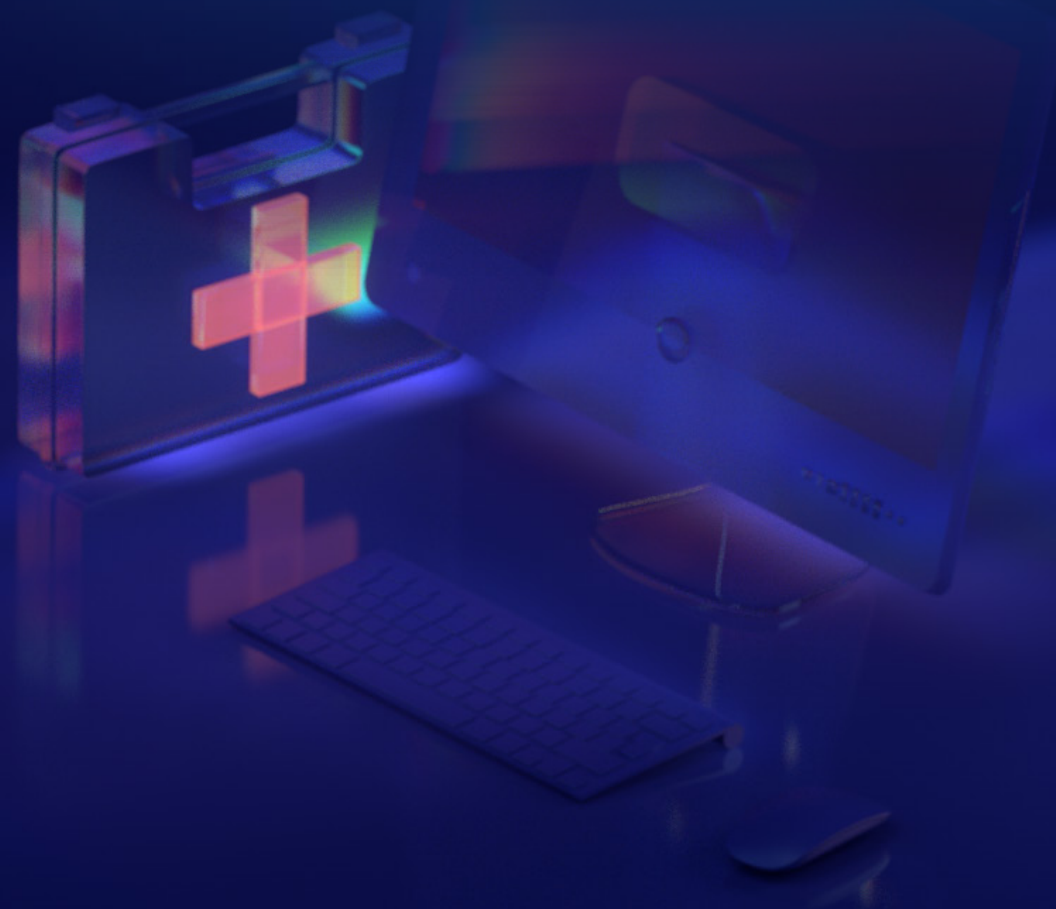
"Cybersecurity incidents have rendered medical devices and hospital networks inoperable, disrupting the delivery of patient care across healthcare facilities in the US and globally."

3 Ransomware

Ransomware is a terrifying and costly threat for healthcare organizations. Hackers essentially take over hospital devices and systems until they're paid to release them. This makes it impossible for doctors and nurses to provide lifesaving care like CT scans, ultrasounds, and more.

According to a threat report from Cylance, ransomware attacks grew three-fold in 2017, with healthcare being affected the most by this increase. There have also been high profile cases of **hospitals paying hundreds of thousands of dollars** to get their data and devices back.

Unfortunately, ransomware attacks have serious health consequences for patients—**one woman in Düsseldorf, Germany died after a ransomware attack** at the closest hospital forced her to be taken to a facility further away.



Healthcare ties for top place in Siteimprove Web Security scoring

We assessed 312 healthcare websites across Europe and North America to find that these sites rank highest (along with government) in their web security scores.

The **overall score for healthcare domains was 80 out of 100**, higher than the average of 78. Healthcare sites also scored well in the server score category, with a score of 80 (the average was 76). This means healthcare sites have secure hosting, data bases, and server setups. They're also well defended against CMS vulnerabilities and SSH vulnerabilities.

Web Security score

Healthcare sites also scored well in the web application category with a score of 66 (the average was 64), meaning they have strong encryption, active certifications and cookies, as well as secure on-page content.

The only category healthcare sites scored below average was in the network category, meaning they're slightly weaker on attacks against malware and phishing.

All in all, it was reassuring to see healthcare sites take web security seriously and protect patient data.

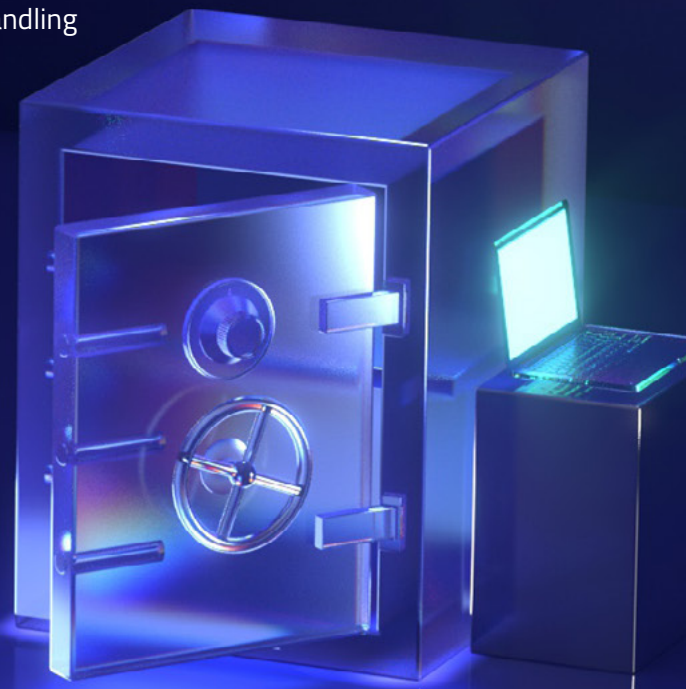
Financial services

Financial services face immense cybersecurity pressure. **As PWC aptly puts it**,

"Criminals target financial firms because that's where the money is.

As with most other sectors, financial services are facing increased threats from coronavirus. **New research claims** there's been a 238% surge in cyber-attacks against banks due to the pandemic.

But coronavirus has only increased an already very high number of threats facing the industry: **The 2020 X-Force Threat Intelligence Index by IBM** found that **the financial services and insurance industry was the most attacked vertical for the last four years**. However, it's one of the best verticals at handling attacks.



In the same study, IBM says "finance and insurance companies tend to experience a higher volume of attacks relative to other industries but are likely to have more effective tools and processes in place to detect and contain threats before they turn into major incidents."

Despite their good track record, the financial services industry still faces very real challenges when it comes to cybersecurity.

Main challenges for financial services

1. **Attacks from within**
2. **Third-party infiltration**
3. **Ever evolving technology**

1 Attacks from within

Financial services are particularly vulnerable to insider threats. **The Harvard Business Review cites a study** that found 60% of all cyber-attacks are carried out by insiders. That same study found that **financial firms and financial services were in the top three sectors targeted by insider attacks.**

While not all insider attacks are intentional (**about 29% of attacks** involve insiders falling for phishing emails), many are. And to be clear, not all attacks come from tenured staff—contractors, temporary workers, suppliers, or business partners that have authorized (but uncontrolled) access to systems can also cause harm. These inside attackers pose a high risk for financial theft or fraud, business disruption, or destruction of critical infrastructure.

2 Third-party infiltration

Many financial institutions rely on third parties for tools and services, including everything from cloud hosting, to HR software, to outsourcing agencies. These tools and services have access to data from those financial services, which opens up an avenue that hackers can exploit. Beyond that, those third parties also use third parties, which can open up even more vulnerabilities.

While third party infiltration is one of the key challenges facing financial organizations, it's not one they're unprepared for.

Nearly **80% of financial services firms** say they would decline, or already have declined, a business relationship due to a third party's cybersecurity performance. The same study found that 97% of respondents say that cyber risk affecting third parties is a "critical" or "important" issue.

3 Ever evolving technology

New technologies allow financial institutions to provide better customer experiences and fuel growth—but they can also function as a weak point for cyber criminals to infiltrate. **As Mindsight writes,**

"In the finance sector, CIOs and CTOs are already considering how blockchain and the Internet of Things (IoT) can be leveraged to build growth."

Unfortunately, **IBM points out** that "the IoT threat landscape has been gradually shaping up to be one of the threat vectors that can affect both consumers and enterprise level operations by using relatively simplistic malware and automated, often scripted, attacks." Already, **61% of organizations have experienced an IoT security incident**.

Unfortunately, **IoT devices are not protected by design**—there is no security standard they have to meet, which means financial services can't secure those devices. That makes the devices (often used for transferring money or customer data) a very easy target for cyber criminals.

Financial services lands just below the top, as ranked by Siteimprove Web Security

The financial service industry scored slightly lower than projected based on their web security readiness. Siteimprove Web Security assessed 1,549 financial services domains across North America, Europe, and Asia, and found they have **an average score of 78 out of 100**. That overall score fell below the top performing industries: government and healthcare.

Their web application score of just 61 clearly prevented them from landing the top spot. Meaning financial services are struggling with weak encryption, expired certificates and cookies, and on-page content vulnerabilities.

However, their network score of 96 and server score of 78 mean they are very well protected against phishing, network attacks, and malware attacks, and moderately protected against CMS and hosting vulnerabilities.

Web Security score

Government

Government entities have made two abrupt changes during the coronavirus pandemic: 1) manage an almost entirely remote workforce, and 2) move all government functions online. While both of those changes will hopefully make life easier for public sector employees and citizens, there is a significant risk that both of those moves will increase cybersecurity threats.

Government entities are hit frequently with cyber-attacks—and unfortunately, **government is one of the verticals least capable of handling attacks**. It's not just the sheer volume of attacks, it's also the severity and significance of the threats.

State-sponsored attacks, miscellaneous errors, and privilege misuse represent 72% of public sector breaches, with **espionage and financial gain reported as the two primary motives**, **according to Verizon's 2019 Data Breach Investigations Report**.

When it comes to reducing the risk of threats, government faces three main challenges.

Main challenges for government

1. **Lack of visibility and oversight**
2. **Behind the technology curve**
3. **Lack of capacity and talent**

1 Lack of visibility and oversight

Concerningly, **only 23% of government entities** say they have sufficient visibility into their attack surface. On top of that, in "38% of government cybersecurity incidents, the relevant agency never identifies the "attack vector," meaning it never learns how a hacker perpetrated an attack," **writes Lily Hay Newman for Wired**.

This comes as no surprise to government—**a White House report from 2018** states that government "agencies' enterprise risk management programs do not effectively identify, assess, and prioritize actions to mitigate cybersecurity risks."

Government entities lack overarching visibility that would allow them to easily detect and report risk. The reasons for why that is are many—including large organizations with many employees, lack of buy-in for web security from top leadership, fragmented reporting and communication, as well as difficulty in rolling out scalable frameworks across entire governments.

2 Behind the technology curve

Government agencies often run on legacy systems, which can pose serious security risks. The Government Accountability Office in the US has said,

"Federal legacy IT investments are becoming increasingly obsolete: many use outdated software languages and hardware parts that are unsupported. Agencies reported using several systems that have components that are, in some cases, *at least 50 years old*."

It will come as no surprise then that Bobby Ford, global chief information security officer at Unilever, said that "legacy IT systems are often at the heart of cyber breach incidents." That makes government particularly vulnerable.

On top of legacy systems, new technology, like AI and the Internet of Things (IoT) pose new challenges that governments aren't often prepared for. **According to a survey by Tenable**, 65% of public sector respondents worry about attacks involving IoT or operational technology (OT) assets. That's a fair concern, given that 55% of the public sector organizations have experienced an attack against IoT or OT infrastructure that resulted in downtime.

The good news is that **63% of government entities want to "improve their ability to keep up with the sophistication and stealth of attackers."**

3 Lack of capacity and talent

According to Deloitte, cybersecurity unemployment is at 0% with more than 1.5 million job openings globally in 2019. The demand for cybersecurity talent is high, which deeply affects government entities, as they have a harder time attracting talent over the private sector.

This labor shortage led to **62% of public sector respondents in one survey** saying that their organizations' security function doesn't have adequate staff to scan for vulnerabilities in a timely manner. Additionally, **wages have steeply increased**, making it difficult for the public sector to compete for talent.

On top of struggling to fill cybersecurity positions, government organizations have a hard time managing the onslaught of threats they currently face. Government entities are hit frequently with cyber-attacks, with the cost per cyberattack estimated to be $1.19 million USD, according to the Global Application & Network Security Report by Radware.

Lack of staff, tools, and resources make it very difficult to manage that volume of attacks.

Government scores among the highest industries ranked by Siteimprove Web Security

Despite being an industry that has historically struggled with web security, government tied for first place along with healthcare when ranked by Siteimprove Web Security.

We scored 2,994 government domains across Central, South, and North America, Europe, and Asia and found government websites have **an overall web security score of 80 out of 100**. They scored highest in the network score category at 96, followed by a server score of 77, but came in at a very low 68 for their web application score.

That means government websites are very protected against malware threats, network attacks, and phishing attempts. They have semi vulnerable website hosting and server setups, as well as high CMS vulnerabilities. These websites are weak on encryption, security certificates, and insecure on-page content.

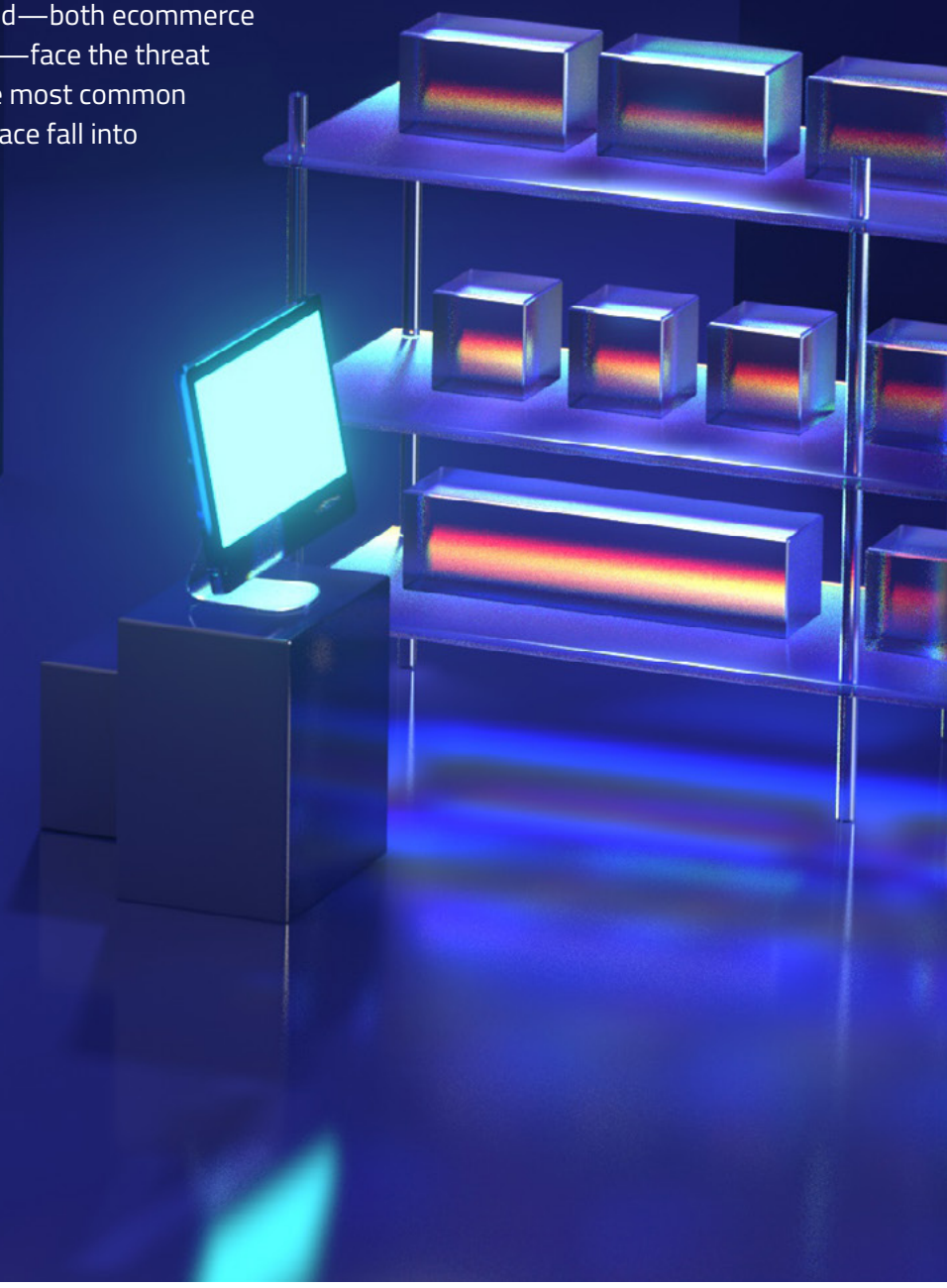
Web Security score

Retail

The retail sector has long experienced a tidal wave of web security threats. **According to IBM**, **retail is the second most attacked vertical after financial services**. **The rate of attacks has increased under the coronavirus pandemic** by 41%. Almost all attacks on retail companies are financially motivated, as attackers attempt to capture and sell credit card details, financial data, or personal information.

The penalty for retail companies who experience a data breach is steep. The average cost of a data breach for retailers in 2019 was $2 million USD, according to the same IBM report. Beyond financial cost, there's also reputational damage, loss of customer trust, and legal action that can follow any breach.

Retailers of every kind—both ecommerce and brick and mortar—face the threat of cyber-attacks. The most common challenges retailers face fall into three categories.



Main challenges for retail

1. **POS vulnerability**
2. **E-skimming**
3. **eCommerce web app attacks**

1 POS vulnerability

POS, or point of sales, are one of the most vulnerable points for any brick and mortar retailer. These devices process hundreds of transactions every day, which contain credit card numbers and PINs. Because these devices contain such sensitive and valuable information, they are naturally a target for hackers, but the devices themselves are actually quite vulnerable.

Often times, retailers don't update their POS software or ensure the device is secure, which leaves it open for malware attacks. Cyber criminals then infiltrate the POS system and steal credit card numbers, PIN numbers, and personal information to sell on the dark web.

Once one POS system is compromised, hackers can move into other POS devices and systems, eventually stealing huge amounts of data.

2 E-skimming

As more and more retail moves online, POS hacking is now taking a backseat to e-skimming or online credit card skimming. E-skimming is when hackers inject malicious JavaScript into payment pages and steal your credit card and personal information—also known as Magecart attacks. **The Oregon FBI says**,

"[E-skimmers] may gain access via a phishing attack targeting your employees—or through a vulnerable third-party vendor attached to your company's server."

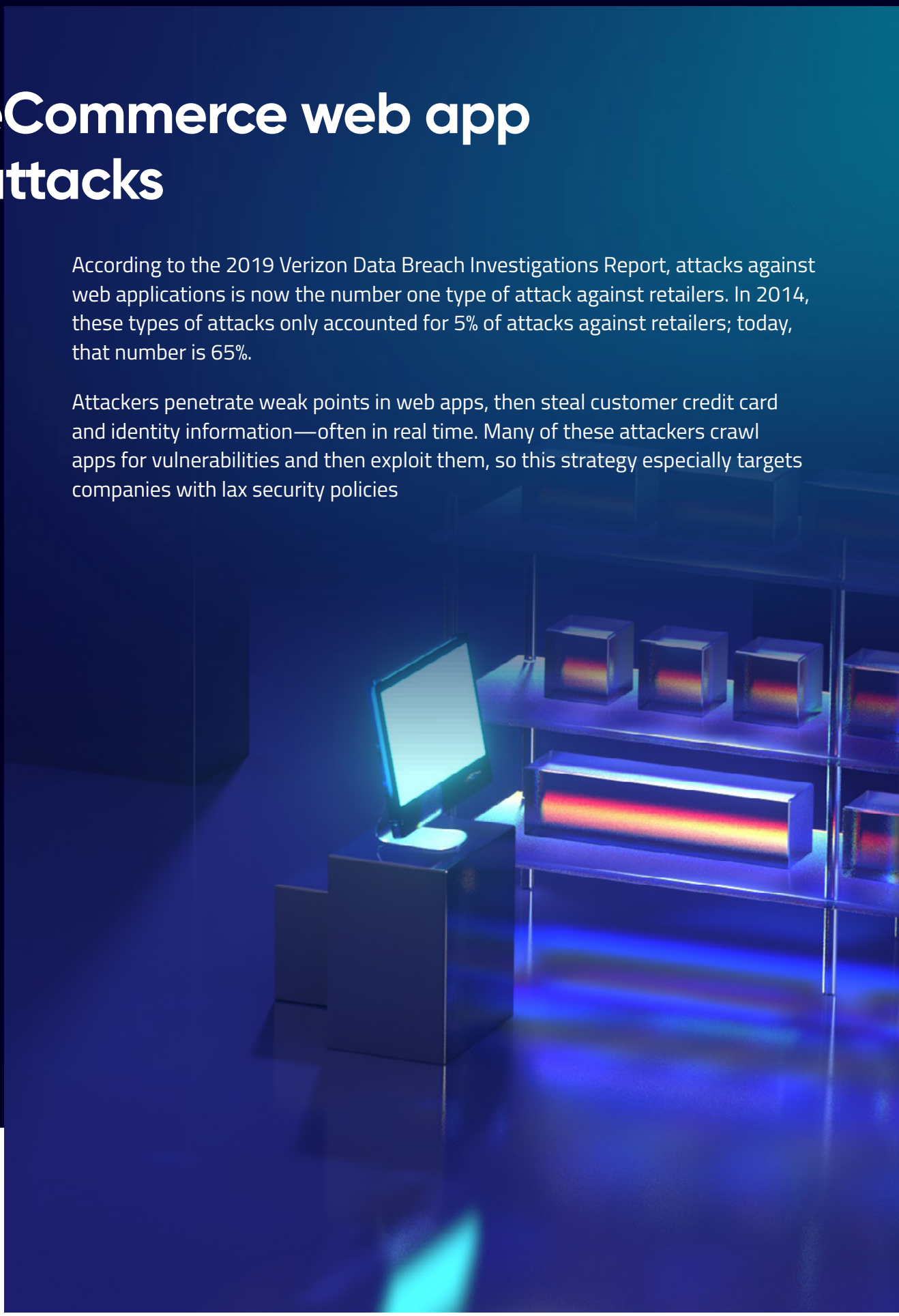
That makes e-skimming particularly complex, because there are many routes cyber criminals can use to gain access to the system.

And unfortunately, this type of crime is on the rise. **In March 2020, the first month of coronavirus lock downs, e-skimming increased by 26%.**

3 eCommerce web app attacks

According to the 2019 Verizon Data Breach Investigations Report, attacks against web applications is now the number one type of attack against retailers. In 2014, these types of attacks only accounted for 5% of attacks against retailers; today, that number is 65%.

Attackers penetrate weak points in web apps, then steal customer credit card and identity information—often in real time. Many of these attackers crawl apps for vulnerabilities and then exploit them, so this strategy especially targets companies with lax security policies



Siteimprove Web Security scores for retail show some concerning trends

We assessed 550 retail websites across Europe and North America and found they had **an average web security score of 74 out of 100**.

Concerningly, **retail had the lowest network score** (89 out of 100), meaning they are the least protected industry against malware activity, network attacks, and phishing attempts.

Their server score of 73 also put them at the lower end of the scale compared to other industries, and indicates they have CMS vulnerabilities, database and server weaknesses, and SSH protocol vulnerabilities. Their web application score of 61 out of 100 put them slightly below the average of 64, meaning they have weak encryption, poor on-page content practices, and potentially expired cookies and certificates.

All in all, retail's web security performance doesn't exactly instill confidence in shoppers when it comes to providing personal and credit card details.

Web Security score

Manufacturing

Dramatic progress in manufacturing technology has, unfortunately, made it susceptible to cybercrime. The birth of the Fourth Industrial Revolution has given us smart factories that run on machine-to-machine learning, integrated devices, self-monitoring, predictive maintenance, and smart sensors. All of these new technologies have led to a dramatic increase in automation and production and a decrease in dangerous working conditions.

However, factories and manufacturing processes that run almost entirely on technology are susceptible to cyber threats. **As IBM points out**, manufacturing data breaches don't often result in exposed information that has to be publicly announced, so it might seem as though the industry isn't attacked that much—**but it is**.

Manufacturing businesses are attractive targets to cyber criminals with financial interests (accounting for 68% of attacks), as well as nation-states that want to cause extreme disruption to a national industry (**espionage accounts for 27% of attacks**).

Manufacturers are all too aware of these threats—**35% of them** even think cyber vulnerability is inhibiting them from fully investing in digital technologies. Generally, their cybersecurity challenges fall into three categories.

Main challenges for manufacturing

1. **Business email compromise (BEC)**
2. **Ransomware**
3. **Supply chain attacks**

1 Business email compromise (BEC)

Because manufacturing businesses interact with many other players (often international ones), business email compromise (BEC) is one of the most popular forms of cybercrime in the industry.

In fact, manufacturing/construction was the most targeted sector in both 2017 and 2018 for BEC crime. In 2019, BEC crime caused **$1.7 billion USD in financial losses in the US alone**.

In these incidences, hackers essentially take over a company's email server or individual accounts, inject themselves into existing email threads, then divert money into accounts they own. Typically, hackers either impersonate:

- Suppliers: Emails often include fake invoices from suppliers
- Employees: Often emails to the payroll department where "employees" ask for their bank account details to be updated
- Executives: Emails that look like they're sent from executives to employees in accounts payable that request money be wired to a specific account for products or services.

2 Ransomware

In 2019, the manufacturing sector paid out **62% of the total ransomware payments**—and it wasn't only large manufacturing companies. Small to medium sized businesses are also hit frequently.

Essentially, **ransomware freezes a company's systems until a ransom is paid to hackers**. Ransomware is typically introduced when an employee clicks on a link or attachment in a phishing email, the threat then spreads to other systems and servers to infect them. After that, there's a request for a payout in order to release systems again.

The biggest threat to manufacturing in a ransomware attack is the complete or partial loss of production time due to systems being frozen. This can cause huge financial loss to a business.

One of the most significant examples of a cyber-attack in the manufacturing sector was the **2017 ransomware attack on pharma giant Merck**. The company had to close down for two weeks and total damages were about $870 million USD. Sadly, Merck's production facilities were also halted, making them unable to produce vaccines.

3 Supply chain attacks

Manufacturing supply chains are deeply complex. At every point in the process, third-party suppliers modify or add products or systems into the mix. At each of those stages, it's possible for bad actors to add malicious software into a product and send it further down the line.

John Suffolk, Huawei's global cybersecurity and privacy officer **points out how complicated the problem is**,

"Our [research-and-development] center for microwave is based in Milan, yet we take our compression algorithms from the world's best scientists and mathematicians in Moscow. And then we apply that to Chinese technology and manufacturing."

As National Defense Magazine comments, "Unfortunately, all along the way, there is plenty of room for bad actors to get into the game of tweaking their aspect of the supply chain to access data that isn't their own."

Manufacturing falls behind average Siteimprove Web Security score

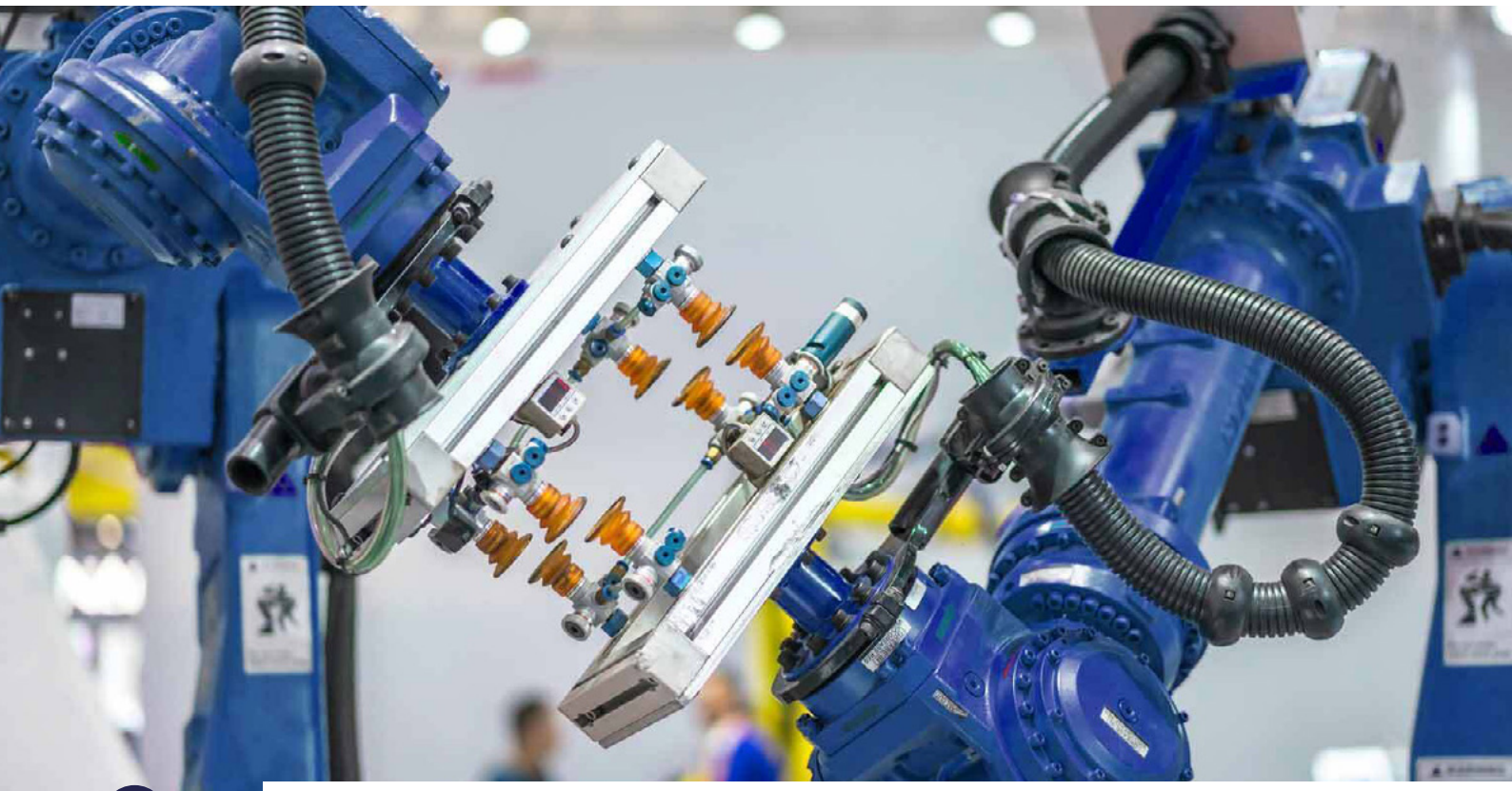
We assessed 526 manufacturing domains across North America, Europe, and Asia and found that manufacturing websites fall behind other industries in all areas. **The average web security score for manufacturing sites was 73 out of 100**, which is slightly below the average of 78.

Web Security score

However, most concerning was the fact that manufacturing scored lowest out of all industries in the web application category. The manufacturing score was 56 out of 100, while the average was 64. This means manufacturing websites have very poor encryption, expired certificates and cookies, and vulnerable on-page content.

These domains did slightly better in the server score category—scoring 72 out of 100 (the average was 76). They scored 90 in the network category (the average was 93). This indicates that manufacturing sites are better prepared for network attacks, malware activity, phishing, CMS and SSH vulnerabilities, but have slightly more vulnerable hosting and server setups.

However, all in all, manufacturing sites performed well below average.



Take control of your web security with Siteimprove Web Security

Exploiting website vulnerabilities is a common first step for cybercriminals. That's why a strong first line of defense involves proactively identifying, categorizing, and managing your website weaknesses. Fortunately, protecting your website, brand, and visitors is easier with **Siteimprove Web Security**.

Siteimprove Web Security simplifies this process by helping you understand and control your website's security with regular, automatic vulnerability audits. These cyberhealth checks are then translated into a single, easy-to-understand score, presented on our signature intuitive user interface.

Armed with your website security score and actionable fixes (prioritized by severity), your team can find vulnerabilities before the cybercriminals do.

Siteimprove Web Security was built with non-specialists in mind to democratize the process of web security. We believe that everyone in your web team should be able to understand web security and do their part to protect your website.

After all, **web security doesn't operate in a silo, it's a critically important aspect of providing a great website user experience.**

Book a 1-1 meeting with our team to learn more about what Siteimprove Web Security can do for your organization.

Book a meeting now

Siteimprove

Siteimprove is a SaaS solution that helps organizations achieve their digital potential by empowering teams with actionable insights to deliver a superior website experience and drive growth.