The state of cybersecurity

Your guide for 2023 and beyond
What we believe

Cyberattacks happen. It may seem easy to ignore cybersecurity and take the “it will never happen to me or my business” stance. We get it—cybersecurity is an overwhelming topic.

That’s why Field Effect exists.

We believe all businesses deserve powerful, cost-effective, and easy-to-use cybersecurity to protect their operations from cyber threats. No matter your security knowledge, resources, or budget, cybersecurity should be approachable and attainable for you.

But where do you start?

We created this eBook to highlight the recent changes in the cybersecurity landscape and share a look ahead to the future. Inside, you’ll find new and emerging threats to watch for alongside other key information that will help you keep your business secure.

More than anything, we want to stop cyber criminals from hurting businesses and people like you. We’ve got your back. If you have any questions, or if there’s anything further we can do to help, please reach out.
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staying ahead of a changing security landscape</td>
<td>4</td>
</tr>
<tr>
<td><strong>How cybersecurity changed in 2022</strong></td>
<td>5</td>
</tr>
<tr>
<td>The Russia-Ukraine conflict’s cybersecurity implications</td>
<td>6</td>
</tr>
<tr>
<td>Ransomeware threats surge</td>
<td>6</td>
</tr>
<tr>
<td>Cybersecurity workforce gap widens</td>
<td>6</td>
</tr>
<tr>
<td>Toolset complexity and alert fatigue</td>
<td>7</td>
</tr>
<tr>
<td>A brief history of cybersecurity tools</td>
<td>7</td>
</tr>
<tr>
<td><strong>Looking ahead: Emerging threats to watch for</strong></td>
<td>8</td>
</tr>
<tr>
<td>Attacks on tools enabling hybrid work</td>
<td>8</td>
</tr>
<tr>
<td>The cybercrime-as-a-service (CaaS) economy</td>
<td>9</td>
</tr>
<tr>
<td>Ongoing ransomware and extortion strategies</td>
<td>9</td>
</tr>
<tr>
<td>Attacks on vulnerable IoT devices</td>
<td>10</td>
</tr>
<tr>
<td>More targeted spear-phishing campaigns</td>
<td>10</td>
</tr>
<tr>
<td>Living-off-the-land (LOTL) attacks</td>
<td>10</td>
</tr>
<tr>
<td><strong>The future of cybersecurity: Trends, threats, and more</strong></td>
<td>11</td>
</tr>
<tr>
<td>Challenges when prosecuting cyber crime</td>
<td>12</td>
</tr>
<tr>
<td>A growing emphasis on social engineering</td>
<td>12</td>
</tr>
<tr>
<td>Greater cyber risks facing the financial sector</td>
<td>12</td>
</tr>
<tr>
<td><strong>Conclusion</strong></td>
<td>13</td>
</tr>
</tbody>
</table>
Staying ahead of a changing security landscape

Year over year, there’s one constant throughout the cybersecurity landscape: change.

Attackers have a frustrating knack for finding new and innovative ways to compromise your business. New tools, technology, and processes on your end may introduce new vulnerabilities that they can exploit.

The cycle continues year in, year out, but it doesn’t mean you should throw in the towel. Far from it, in the spirit of a new year, let 2023 be the start of stronger cybersecurity habits and practices. As new exploits and attack techniques arise, taking a more holistic outlook of your security will help you stay miles ahead of the bad guys.

Before we dig into that approach, though, let’s start by looking back on the dramatic cybersecurity changes from last year.
How cybersecurity changed in 2022

There are no two ways about it:

2022 was a tough year in all things cybersecurity. With most concerns about remote and hybrid work relatively unchanged from the previous year, 2022 initially seemed like it would follow established trends, with new developments emerging gradually as time went on. Hindsight is always 20/20, though, and 2022 rapidly became another banner year for cybersecurity concerns.

Critical infrastructure remained a theme in 2022, as major attacks on vital services like healthcare rose sharply and high-profile incidents made headlines everywhere. Elsewhere, the demand for talented security professionals rose sharply, and issues from years past remained frustratingly persistent.
The Russia-Ukraine conflict’s cybersecurity implications

Unfortunately, 2022 began with major changes that had wide-reaching implications in the form of the Russia-Ukraine conflict. After nearly two months of tension, Russian troops amassed on the Ukrainian border invaded, leading to a widespread and prolonged conflict. The invasion was preceded by coordinated cyberattacks on 70 Ukrainian government websites, compromising 10 and defacing them with threatening messages; further activity targeting Ukrainian systems involved a wiperware campaign in February 2022.¹

Russian cyber activity remains largely focused on Ukraine; however, the ongoing conflict presents an increased cybersecurity risk and concern for many organizations worldwide.

Ransomware threats surge

In April of 2022, Costa Rica experienced two crippling cyberattacks courtesy of the Conti ransomware gang. These attacks targeted essential services in the country, impacting everything from medical appointment systems to scheduled tax payments, leading to the exposure of an alleged 850 gigabytes of governmental data on top of lost millions.²

The Costa Rican government declared a state of emergency in response to these ransomware attacks, the first time a government has taken such an action in response to a cybersecurity incident.

Cybersecurity workforce gap widens

Globally, the cybersecurity workforce grew by 11.1% year over year,³ and yet demand for skilled security professionals continues to outpace the supply of talent. The reasons for this are frustratingly mundane: it takes time and resources to build cybersecurity expertise, both of which are hard to come by for many organizations facing the rising tide of cyberattacks.⁴
Attacks on healthcare rise

The Federal Bureau of Investigation reported that 25% of ransomware attacks in 2022 targeted the healthcare sector. Cybersecurity concerns have been nearly as urgent as the COVID-19 pandemic response for healthcare providers as attackers continued to take advantage of the distractions and uncertainty around continued COVID-19 management.

The majority of major healthcare breaches in 2022 were the result of compromised third-party vendors, however, leading to greater scrutiny over organizations’ digital supply chains. By no means exclusive to the sector, cybersecurity in the digital supply chain is a theme that began to draw greater attention throughout the year that was.

Toolset complexity and alert fatigue

One thing that didn’t change? Toolset complexity and alert fatigue. More tools don’t necessarily result in a better security response. In fact, companies with a more complex tech stack often have a harder time detecting and responding to an attack.

That’s because complex toolsets create noise that becomes easier to tune out over time, leading to what’s known as alert fatigue. Imagine dealing with hundreds of alerts from multiple security tools at any given time and sifting through reams of data to try and figure out what’s a genuine threat and what’s a false positive.

Adding new technology to manage security has quickly become an outdated approach. Each new tool is another budget line item, and growing toolsets demand even more time to oversee. Each tool may only provide a view into one aspect of your IT environment, resulting in a siloed approach to threat management. What’s more, integrating new tools is another time-consuming task; finding interoperable tools that scale to your security needs is tough.

The shift to hybrid work has only made this more apparent, with additional challenges from the use of shadow IT solutions—tools and software that an IT team doesn’t have total control or knowledge of—that staff may put in place to support their new work setup.
For years, threat actors have been mirroring technological changes, tweaking and refining their attack tactics to achieve greater success. As someone with a pivotal role in securing private company data and systems, you know how critical it is to stay on top of new and emerging risks. As you look to the future to update your company’s defence this year, keep these seven cyber threats top of mind.

**Attacks on tools enabling hybrid work**

As companies have adjusted to the modern hybrid work environment, we witnessed a stark increase in the adoption of remote access tools, video conferencing apps, and cloud-based services.

Our cybersecurity analysts anticipate that threat actors will continue exploiting this expanded threat surface. They may focus their attacks on:

- Remote desktop apps
- Misconfigured web-based services
- Legacy operating systems
- Unpatched internet-facing applications
- Outdated browsers

We may also see a focus on serverless attacks as organizations continue adopting the cloud-service model.
The cybercrime-as-a-service (CaaS) economy

Another top cyber threat is the flourishing CaaS economy. It’s never been easier for criminals with little to no technical experience to access these increasingly sophisticated marketplaces, meaning that anyone with malicious intent can now stage an attack with relative ease.

Our team agrees that threat actors will continue participating in criminal online marketplaces, renting and selling items such as:

- Phishing and exploit kits to gain initial access to victim systems
- Stolen account credentials to impersonate a legitimate user
- Databases of confidential personal and corporate information
- Ransomware services and malware to encrypt and extort victims
- Infrastructure to run the malware

Why is this a top threat? Despite extensive efforts to take down these online marketplaces, they still exist. This ability to buy and rent malware means anyone—even those with little to no experience—can become a cyber criminal.

We may see attacks increase as threat actors capitalize on a highly scalable income stream and the fact that they no longer need a technical skillset to hack systems. They can simply buy or rent the tools to carry out their attack, and at a low price too.¹¹

Ongoing ransomware and extortion strategies

Most companies have realized the importance of properly backing up data in case they’re the victim of a ransomware attack. But there’s a new extortion technique that renders these efforts insufficient.

Attackers start by doing their homework—researching the target’s assets and financials—and use this intel to set a ransom fee. Then, instead of encrypting the data and offering a decryption key in exchange for money, they threaten to release sensitive information publicly if the victim doesn’t pay.

They coerce the target into paying by threatening to cause a data breach, a technique that exploits new privacy regulations¹² that penalize companies for not properly securing private data. Attackers depend on the fact that their ransom may cost less than the penalties, fines, and reputation damage the company may face if they choose not to pay.

To stay safe, remind employees that they are a target and can defend themselves by remaining vigilant and following cybersecurity best practices,¹⁰ such as:

- Patching software regularly
- Using strong passwords
- Backing up data regularly
Attacks on vulnerable IoT devices

Internet of Things (IoT) devices — such as smart security cameras and thermostats — are quickly becoming a valuable target for attackers. Our team anticipates this trend will continue.

IoT devices connect to networks, cloud apps, and other technologies, and offer endless productivity benefits for businesses and individuals alike. They’re helping create an increasingly connected world and will likely become even more commonplace as people integrate IoT into their day-to-day lives.

Unfortunately, these devices are often connected to valuable company assets but are rarely built with security in mind. Weak security controls on these devices are a major concern, especially as they share a network with systems and devices housing highly sensitive information.

And while IoT manufacturers have started to focus more on incorporating security controls, many still prioritize functionality and affordability.

More targeted spear-phishing campaigns

Phishing continues to be one of the easiest, cheapest, most popular cyberattack methods, and we expect it will remain a top cyber threat in 2023 and beyond. But to ensure success and a higher return on investment, attackers may become more selective while choosing their victim. This is spear-phishing.\(^{13}\)

Thanks in part to the CaaS economy and phishing-as-a-service offerings, attackers can spend less time developing tools and more time researching their targets. They may form their attacks using personal information gained from social media accounts and company websites to create more convincing spear-phishing campaigns.

Attackers may target specific groups, such as:

- Online retailers, as they may operate on unsecured e-commerce platforms
- Virtual education platforms, due to the increasing number of users
- Healthcare institutions, as they collect a lot of sensitive data and, due to the critical nature of their business, may be more likely to pay a ransom

Living-off-the-land (LOTL) attacks

We expect LOTL attacks to remain a top cyber threat. Despite being mainstream for many years already, LOTL attacks often go undetected for long periods. These attacks make use of tools already installed on targeted computers — instead of uploading and executing custom malware, for example — a feature that makes them challenging to defend against.

Because they don’t generate any new files, attackers can fly under the radar of many security tools and cause significant amounts of damage. Consider this as you add or swap out security solutions this year. Covalence\(^{14}\) is one example of a cybersecurity platform intelligent enough to spot a wide range of threats and vulnerabilities, including discreet LOTL attacks.
Speculating on the future of cybersecurity is inherently challenging. From new attacks and techniques to technology and defenses, it’s always changing and evolving. Still, our team of cybersecurity analysts have provided their best insights on what the future may hold, looking beyond this calendar year.

In the next five to ten years, prevention and preparedness will be more vital than ever. If 2022 taught the cybersecurity industry anything, it’s that proactively planning for a cybersecurity incident or data breach is critical. Expect to see a greater emphasis on preparedness and response playbooks, not to mention growing investment in employee education and training at all levels.

What’s more, evolving privacy and security concerns are expected to become far more urgent as laws come into full force. Beyond the European Union General Data Privacy Regulation (GDPR), Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA), and the California Consumer Privacy Act (CCPA), additional state- or region-level regulations are being introduced at a rapid pace. The greater scrutiny of cybersecurity controls could lead to further impacts for In-scope companies and organizations.

Companies that work with personally identifiable information should prioritize compliance moving forward. Ensuring cybersecurity programs comply with existing or forthcoming regulations and align with accepted frameworks is and will continue to be a top-of-mind concern.
Taking a look beyond the next 12 months, a few threats and trends are apparent that will likely play a bigger role:

01 Challenges when prosecuting cyber crime

Despite the growing number of countries actively regulating data privacy and cybersecurity, prosecuting cyber crime may still prove difficult in the future. A lack of attributable data and evidence for alleged criminal acts conducted online will make it harder for law enforcement to effectively prosecute criminals.

This challenge will be exacerbated by an ongoing shortage of cybersecurity professionals, which will make it that much harder to accurately identify potential cyber threats.

02 A growing emphasis on social engineering

Although security solutions are more robust and powerful than ever before, they still face a major challenge: human error. In the coming years, internet communications will likely become more secure, especially as technology evolves to reduce the relevancy of network-based threats.

Nevertheless, the human element remains. Users can and will continue making mistakes that lead to data loss. Attackers will still attempt to lure users into taking actions that could compromise security.

03 Greater cyber risks facing the financial sector

As payment systems are modernized, financial transactions may become entirely digital. This transformation will usher in a wide range of platforms and methods to conduct financial transactions.

This diversity will likely expand the threat surface for financial institutions and platforms, increasing the likelihood of fraud-based attacks targeting digital currencies, the blockchain, and real-time payment solutions. What’s more, because of their decentralized nature, regulatory bodies will take some time to catch up and enforce compliance activities.

It’s hard to look at the calendar and make predictions about what the future will hold, especially in an industry as complex and fast-paced as cybersecurity. But by taking the time now to build that foundation, you can set your business up for lasting success as changes arise and new threats...
Conclusion

We hope this eBook has given you valuable insight into the future of cybersecurity.

If you take only one thing away from what you’ve read, we hope it’s that businesses like yours are facing very real, ever-evolving cyber threats.

While it’s extremely important to have cyber insurance and backups, you can’t rely on just these to prevent an attack. The primary focus for businesses looking ahead should be, first and foremost, on securing their operations now. Proactively securing your company against emerging risks can help prevent cyberattacks and save your business.

Remember, you’re not alone. It’s our mission to help protect small and mid-size businesses. If you have any questions, or need any help with your cybersecurity, get in touch with our Field Effect team.

We’ve got your back.

SOURCES

8. [https://fieldeffect.com/blog/the-threat-surface/](https://fieldeffect.com/blog/the-threat-surface/)
The most sophisticated cyber threat monitoring on the planet, made simple.

Covalence is an award-winning cybersecurity solution that provides transparent, holistic managed detection and response for your whole IT infrastructure in one platform, no matter where you are or where your endpoints are located. No add-ons, no modules, and no gaps in your security. Learn more about Covalence.

About Field Effect

Field Effect believes that businesses of all sizes deserve powerful cybersecurity solutions to protect them.

Our threat monitoring, detection, and response platform, along with our training and compliance products and services are the result of years of research and development by the brightest talents in the cybersecurity industry. Our solutions are purpose-built for SMBs and deliver sophisticated, easy-to-use and manage technology with actionable insights to keep you safe from cyber threats.

Contact our team today.

Email:
letschat@fieldeffect.com

Phone:
CANADA + UNITED STATES  
+1 (800) 299-8986
UNITED KINGDOM ... sophisticated, 
easy-to-use and manage technology with actionable insights to keep you 
safe from cyber threats.
[49x222]About Field Effect
[49x210]Field Effect believes that businesses of all sizes deserve powerful cybersecurity solutions to protect them.

Our threat monitoring, detection, and response platform, along with our training and compliance products and services are the result of years of research and development by the brightest talents in the cybersecurity industry. Our solutions are purpose-built for SMBs and deliver sophisticated, easy-to-use and manage technology with actionable insights to keep you safe from cyber threats.

Contact our team today.

Email:
letschat@fieldeffect.com

Phone:
CANADA + UNITED STATES  
+1 (800) 299-8986
UNITED KINGDOM ... sophisticated, 
easy-to-use and manage technology with actionable insights to keep you 
safe from cyber threats.