2020 CYBERSECURITY FORECAST

TOP 10 EMERGING BUSINESS THREATS

The Swenson Group
People · Passion · Purpose

2020 CYBERSECURITY FORECAST

Although the future of new technology is promising on so many levels, new technologies and the evolution of existing technologies continue to positively impact businesses. However, while there are many great things coming on the horizon, 2020 will most likely see an inordinate rise in the number of security breaches, attacks and incidents.

Risk mitigation is rising among business priorities.

This guide is intended to help business leaders prevent avoidable data breaches with a heightened awareness of the everchanging cybersecurity landscape in the year ahead.

TOP 10 Business Threats and Predictions

#1 The Continuing Rise of "Deepfake" Technology.

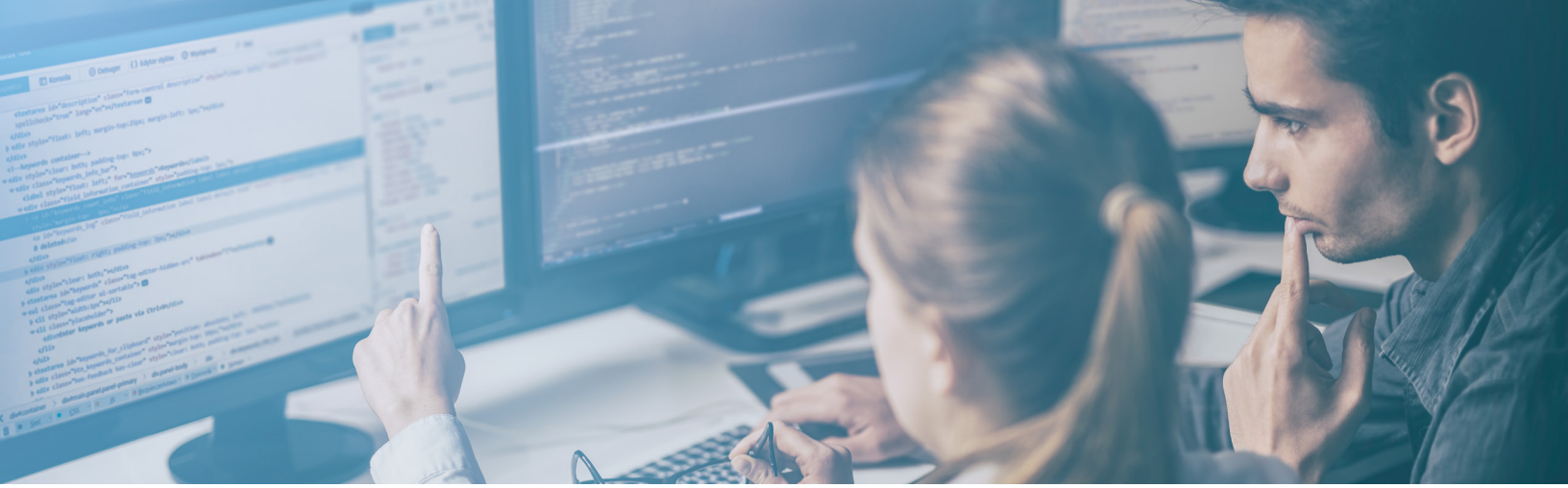
Deepfake technology is an AI-based technology that was created to produce and alter video content so that it appears something occurred, when in reality, it didn't. Deepfake technology is here to stay, and its use against businesses and in misinformation campaigns is predicted to continue growing throughout 2020. In fact, the problem is expected to become so pervasive, Gartner predicts that "by 2023 up to 30% of world news and video content will be authenticated by blockchain, countering deepfake technology."

#2 A Shift Toward Multi-Factor Authentication (MFA).

Two-factor authentication (2FA) has become prevalent as a security measure in the past couple of years. In 2020 authentication will move from 2FA to multi-factor authentication, including biometrics, according to predictions by Lookout security experts. Moving forward, companies are increasingly adopting MFA and biometrics using mobile devices to protect against credential theft and address regulatory compliance.

#3 Improvements in Facial Recognition Technology.

Google's release of Pixel 4 proved it can compete with Apple's facial recognition technology, but it won't stop there. Google will continue to update this technology to make it the most secure biometric tool on the market. Starting with its flagship devices and then trickling down to mid-priced consumer tech, nearly all smartphone OEMs will depend on facial recognition by the end of 2020. Facial recognition will also be deployed for desktop and laptop computers.



#4 Hackers Will Shift Their Focus to the Cloud.

As more business has migrated to the cloud, so has the focus of cybercriminals. The good news and bad news... staging an attack will become harder but the actions of criminals will become more sophisticated and more frequent. According to a Kaspersky look at 2020 security trends, hackers will begin to rely more on chance rather than planning attacks.

#5 Insider Attacks Will Increase.

A rise in insider attacks is forecast for 2020 due to the high cost of executing malware-based attacks. Direct infrastructure attacks are becoming much more difficult, expensive, and require more skills and time for the attacker to be successful. The human factor is typically the weakest link in security strategies and structures. As a result, we'll see a growth in attacks that use social engineering methods. Attackers will pay large amounts of money to insiders for information and access.

6 Smarter AI Attacks.

Hackers now have access to AI and will use it in two different ways. First, they'll use AI to more easily breach networks. A hacker will code a hackbot using AI and release it onto the web. The hackbot will attempt to breach a network, fail and learn. The next time it will succeed and the bot will continue to learn until it is unstoppable. The second way they'll use AI is to attack the target company's AI tools while they're still in the learning stage, making it possible to use their AI tools against the company, breaching their network.

#7 Growth of Edge Computing Attacks.

The worldwide adoption of 5G technology will begin in 2020. This will provide an uptick in edge computing and many new IoT connected devices. Unfortunately, many are left unprotected. More than 70% do not mandate authentication of third-party APIs, and more than 60% do not encrypt data. This lack of controls makes these devices easy prey for a hacker who can not only steal data but can also infect these devices with bots or malware. If an attack isn't immediate, it could go unnoticed for months, or years. Plus, 5G networks will allow these delayed attacks, when triggered, to happen with amazing speed and efficiency.

8 Increased Use of Collaboration Tools as a Point of Vulnerability.

Collaboration suites and tools will become more attractive to cybercriminals. Tools like Zoom and Microsoft Teams can become new avenues for attack. As more organizations increasingly use these types of tools, they will need to keep up to date with cybersecurity to address their vulnerabilities. More than 75% of enterprises will have security specialists focusing on these collaboration tools by the end of the year.

#9 Need for Trained Cybersecurity Talent.

In 2017, the World Economic Forum reported a shortage of trained cybersecurity specialists. The shortage has increased in the past two years. It's been projected by Cybersecurity Ventures that there will be 3.5 million unfilled jobs worldwide by 2021, up 350% since 2014. There are nearly 1 million cybersecurity workers in the US and there are still roughly 500,000 unfilled positions. The number of security-training companies and certifications is growing and employment is almost guaranteed for qualified applicants.

#10 Heightened Focus on Employee Training.

When it comes to preparedness, it's not just about technology. Organizations need to prioritize security best practices to ensure they remain safe. It's important for IT teams to have up-to-date knowledge to prevent and prepare for security threats they may face in today's hostile landscape. Training is one of the easiest and most effective ways to keep your organization secure. The threat landscape is constantly changing and it's vital to keep employees aware of the latest security protocols.

From deepfake technology, to the cloud, to the Internet of Things, in the coming year nothing will be safe from attack. While it's a key to stay on top of the latest strategies, risks, and threats, the silver lining is that while attackers are growing more sophisticated, the cybersecurity industry is becoming more robust to thwart these threats.

The Swenson Group
People · Passion · Purpose

About The Swenson Group (TSG)

The Swenson Group specializes in providing business technology products and services to mid-size businesses. Clients can Control Technology Related Costs, Improve Employee Productivity, and Secure Hardcopy / Digital Data. In 2019, TSG was recognized multiple times for customer service excellence.