NETWORK PROVIDERS, INC.
JULY 2023

Cybersecurity TECHNOLOGY

NEWSLETTER

How to Stay Ahead of AI-Powered Cybersecurity Risks

BY JAY HILL

President & CEO

I am thrilled to announce the launch of NPI Tech Magazine this month. We will be using the publication as a vehicle to bring local business owners together. It will serve as a platform to showcase our expertise, share insightful perspectives, industry trends, and foster a deeper understanding of the ever-evolving technology landscape. It will feature thought-provoking articles, in-depth interviews with business leaders, expert analyses, and captivating stories that highlight the latest advancements and breakthroughs across various industries. As a valued customer, you will receive a copy by mail in the coming weeks.

It is important to acknowledge the valuable contributions made by our employees for their relentless pursuit of excellence. The passion, dedication, and unwavering commitment displayed by each member of our incredible team have propelled us forward, and it is your collective efforts that deserve every ounce of recognition. Together, we will continue to embrace change, explore new opportunities, and stay at the forefront of our industry.

Thank you for all you do!

While artificial intelligence (AI) has many benefits for businesses, it has also created new vulnerabilities that cybercriminals can exploit to carry out complex cyberattacks that are difficult to detect and mitigate. Using AI, hackers can create convincing phishing emails that bypass spam filters. Similarly, cybercriminals can leverage AI to manipulate security systems and gain unauthorized access that causes irreparable damage to your business and your reputation.

This emerging threat landscape can be tough for businesses that do not have a dedicated IT security team equipped with the advanced tools to mitigate complex cybercrimes. Fortunately, there is a lot you can do to bolster your organization's cybersecurity. We'll explore ways to improve your preparedness against AI-powered cyberattacks.

Security Best Practices For AI

Here are some practical tips for enhancing your organization's cybersecurity posture against emerging AI threats:

Provide continuous, real-time cybersecurity training for your team

AI technology is evolving quicker than ever, and so are cyberthreats. Mix the two together without continuous cybersecurity training for your team and you'll have a security disaster on your hands.

When a hacker targets an organization, an employee often gets blamed for clicking the wrong link or downloading an infected file. However, rather than blaming an individual, devise a strategy to ensure all your employees have the knowledge and training they need to make the right decisions.

For example, you can use real-time scenarios or simulations to help your employees identify phishing emails so they don't fall for malicious attempts. You can even set up regular, ongoing security awareness training to educate your employees about persistent threats like ransomware and social engineering attacks. If you want your employees to embrace good cybersecurity habits, you have to build its importance into the company DNA.

Improve security policies and enforce them

As AI-powered cyberthreats evolve, take proactive steps to improve cybersecurity policies and enforce them rigorously through consistent communication that emphasizes the necessity of good cyber hygiene. Your IT and HR teams can also work on cybersecurity strategies and policies that ensure your employees stay vigilant and aware of the latest AI cyberthreats. For example, you can have weekly newsletters sent out to employees to keep them updated on emerging threats.

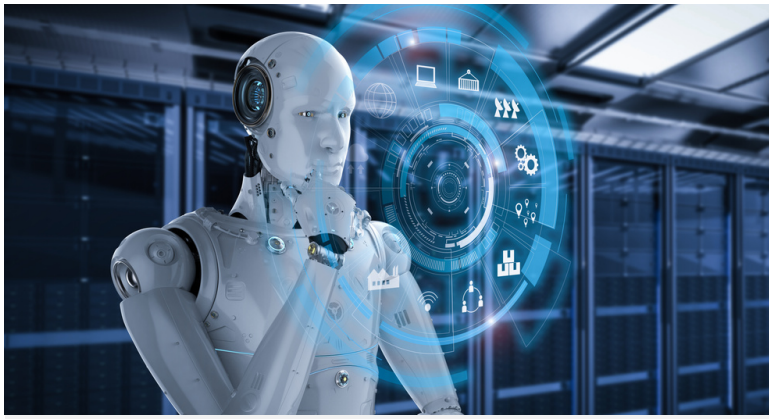
Additionally, you can carry out regular risk assessments and implement multifactor authentication to enhance your cybersecurity. Businesses that don't

Continued from pg. 1

have IT teams or security resources have been able to build a strong IT security stance with the help of a trusted IT service provider.

Partner with an IT service provider
An experienced IT service provider will have the inside scoop on all the latest developments in AI and can help you build a formidable cybersecurity posture that protects your business from AI-related threats. Since an IT service provider has the advanced resources and tools to combat threats, you can focus on crucial business decisions without having to worry about managing your IT security.

We are here to help
Make cybercriminals the least of your worries. Consider partnering with an IT service provider like us. We have the experience and expertise to help you build a solid cybersecurity posture against AI-fueled security threats without breaking the bank. Contact us today!



Did You Know?

Artificial intelligence was a concept invented in the 1950s by computer scientist John McCarthy. Since then, it has become a cornerstone of modern-day technology. AI is now being used to automate mundane tasks, improve customer service and even provide medical diagnoses. The list of what AI can do is endless — it's no longer just a concept but a reality that can benefit and improve our lives.

##

#BeCyberSmart
#FightThePhish

Get More Done in Less Time

Tech Tips To Improve Productivity And Focus

Technology has become essential to our society. We use it for nearly every aspect of our lives, from entertainment to personal security. Unfortunately, it's not all good, and over time, many of us have developed some negative tech habits. When we're supposed to work or stay productive, we might turn to our phones or tablets and scroll through social media or the news. There's no better time than the present to shake these harmful habits so we can become more productive. The good news is that technology can actually help improve our overall productivity.

The pandemic forced many of us to start working remotely or in a hybrid environment, which makes it even more important for us to use technology to stay focused and productive. Technology does not have to be a distraction: it can help us stay on task and achieve our goals. Below, you'll find a few ways to use technology to improve productivity.

Cleaning Up Your Digital Space
For many of us, our workdays revolve around our electronic devices. We spend nearly eight hours each day bouncing from our computers to our cell phones, trying to stay in touch with everyone while keeping up with our workload. Over time, our digital areas can become cluttered with unnecessary documents, e-mails and other information.

Instead of creating job descriptions, I encourage colleagues and clients to follow a practice called writing a "scorecard." A scorecard has a clear mission for the role. It identifies 5–7 outcomes you expect a person to achieve by a specific date. The outcomes are a mixture of actions you want the person to take and the results you expect them to achieve. This makes it easy to "score" whether someone has achieved the outcomes. Using a scorecard will improve your ability as a leader to hire and coach people to embody the organization's purpose and take actions that achieve results.

Take time to review and reorganize your computer's desktop, smartphone's home screen, e-mail inbox and cloud storage accounts. Delete any unnecessary files, e-mails and apps you no longer need. By doing this, you'll have an easier time navigating through your digital space and locating necessary documents when they're needed.

Using Time-Tracking And Focus Apps
Time can easily slip away from us if we're not paying close attention. We've all gotten lost in a project or task and spent way too much time on it. One of the best ways to stay focused and productive is to track your time. Many apps are available that help you do this, including Toggl, RescueTime and Harvest. These apps allow you to track how much time you spend on specific tasks and can help you identify where you might be wasting time. By tracking your time, you can make adjustments to your schedule and ensure you're making the most of your hours.

Focus apps like Freedom, Cold Turkey and SelfControl can also help you stay productive, as they'll ensure you aren't wasting your time on social media or other websites that take you away from your work. These apps allow you to block access to certain websites or apps for a specified amount of time. In fact, using a focus app is one of the best ways to remove distractions from your workday.

Automating When Possible
Automation has truly revolutionized the way many businesses operate. You can use automation for e-mail communication, marketing efforts, data collection and so much more. Introducing automation to your business can help streamline repetitive, time-consuming tasks that previously had to be done manually. By automating various processes and functions, you'll free up more time for your employees to focus on higher-level tasks and improve their productivity. Automated systems are also less prone to errors than human beings, so you won't have to spend as much time going back through your work to fix simple mistakes. Automation improves productivity by reducing the time, effort and resources needed to complete a task, while providing valuable data insights.

Strengthening Your Cyber Security Practices
A successful cyber-attack can completely dismantle your business. It can take days, weeks or even months to recover from a cyber-attack, which can put an end to your hopes of improving productivity.

Facebook Owes You Money!

How To Apply For Your Share Of Facebook's Recent $725 Million Privacy Lawsuit

Here's a shocker: Facebook is being forced to pay a whopping $725 million in a settlement following a number of lawsuits claiming they violated users' privacy. This is in addition to another class action lawsuit for $650 million for storing and collecting the biometric data of nearly 1.3 million Illinois residents without their knowledge or consent.

The lawsuits allege that Facebook shared data from users and their friends with third parties without the users' knowledge or consent and then failed to monitor or direct how these third parties accessed the data or what they did with it.

The plaintiffs' lawyers estimate about 250 to 280 million people may be eligible for payments as part of this suit.

The money being paid to each person depends on how long they've had a Facebook account and how many people actually file claims. Users will get "points" for every month they've had an account between May 24, 2007, and December 22, 2022. The money will be split (after lawyers' fees are paid, of course) based on those numbers, so don't expect a financial windfall that will allow you to move to Beverly Hills. The only people getting rich here are the lawyers.

If you had a Facebook account during the dates above, you're automatically part of the settlement, but you must submit a claim by August 25 of this year. If you do nothing, you won't get paid and you'll give up the right to sue or be part of another lawsuit against Facebook related to these claims.

However, if you're feeling ambitious (and have deep pockets to pay the legal fees), you can choose to opt out of this lawsuit and attempt to sue Facebook separately, under your own initiative.

We should all be happy that big tech companies accessing, selling and sharing our data without our knowledge or consent are being held accountable; but it's not enough to depend on lawyers or our government to protect our identity and personal information. Companies like Meta make far too much money from our data to turn away from selling it and using it.

For example, Meta made over $116 billion last year from a FREE app. That money is coming from selling access and data. This lawsuit, while sizeable, only represents just 0.62% of the company's total revenue – a rounding error.

The entire dark web and the rise of hacking demonstrate how much money there is to be made from gaining access to personally identifiable information, so you need to be careful you don't end up a victim of your data being stolen, shared and sold.

One of the ways to prevent your information from being shared is by going into the privacy settings on Facebook and finding "Your Facebook information." From there, click "Off-Facebook activity" and "Recent activity" to clear your history.

You can also click "Manage future activity" and choose "Disconnect future activity" to disable this feature. Of course, if you like the ads you get from Facebook this will (should?) make all of that go away.

Another suggestion is to check the privacy settings on your phone to ensure apps installed aren't getting free access to your camera and microphone unless specifically given permission by you to perform those functions. Many apps will install with that access feature turned on and require you to opt out.

Of course, as a business owner, YOU have to also think about how you are storing and using your clients' data. As this lawsuit proves, the government is taking data privacy and protection seriously, which is why you're seeing more regulatory compliance for data security and privacy hitting all industry sectors.

If you want to make sure you're not accidentally exposing your clients' data and violating data protection laws, schedule a quick call with us to discuss your concerns and see if there are ways we can help you avoid exposing your clients' and employees' data by accident.

The Interim DFARS Rule and What It Means for You

The Cybersecurity Maturity Model Certification (CMMC) was formally made part of the Defense Federal Acquisition Regulation Supplement (DFARS) in January 2020 and updated to CMMC 2.0 in November 2021. The decision affected more than 300,000 defense industrial base (DIB) members, and many found themselves drowning in all kinds of unnecessary noise surrounding CMMC and its implications on existing and future government contracts.

The chaos increased when the Interim DFARS Rule (DFARS Case 2019-D041) joined the foray on November 30, 2020. This rule mandates all defense contractors to perform cybersecurity self-assessments using the NIST CSF (SP) 800-171 DOD Assessment Methodology to qualify for new defense contracts and renewals of current contracts.

Amid all the deliberations and scrutiny, let's try to understand the Interim DFARS Rule and its impact on you as a member of the DIB. In this blog, we'll discuss what's changed in the Interim DFARS Rule, what it mandates contractors to do and what your next steps should be with this latest mandate by the Department of Defense (DOD).

What changed in the Interim DFARS Rule?

This is not the first time the DOD has emphasized the need for defense contractors to follow the 110 cybersecurity controls defined in the National Institute of Standards and Technology (NIST) Special Publication 800-171, generally referred to as "800-171."

Even before the adoption of CMMC, DFARS mandated that most defense contractors merely attest that they followed all the controls specified in 800-171. However, many non-compliant contractors and sporadic government audits led to controlled unclassified information (CUI) being leaked.

In an effort to counter potential security threats, the Interim DFARS Rule requires contractors to complete self-assessments and formally score their 800-171 compliance status based on a specific scoring system developed by the DOD. The contractors must then upload the self-assessment score to a federal Supplier Performance Risk System (SPRS) database to qualify for new contracts and renewals.

Continued from pg. 3

What Does Independence Day Mean?

Independence Day, or Fourth of July, Anniversary of the adoption of the U.S. Declaration of Independence by the Second Continental Congress (July 4, 1776). It is the greatest secular holiday in the country. Celebrating the day became common only after the War of 1812. Declaration Of Independence and The Preamble of the Constitution are standalone documents that should remind us that All Means All and not some. As Americans, we get to take stock of where we have been, where we are, and where we are headed.

Independence day remind us of our country's heritage either good, bad, or indifferent. We must continue to fight against the tyranny of injustice, inequality, and denial of basic necessities and rights for those who go without and are on the margins of society. Under one nation, we need to get back to the basics and not be suspicious and hateful towards others. We must continue to educate and re-educate ourselves by going back and study American History and Government.

The 4th of July means that we get to remember the men and the women who lost their lives by taking a risk to break free from a foreign despot in order to form a new nation.

We must give thanks for our lives, liberty, and "The Pursuit of Happiness.

What does this national holiday mean to you and your family?

That's a good question to ask to each other and for us to ponder on this Independence Day.

Now that you understand the crucial changes in the Interim DFARS Rule, let's discuss how the rule's scoring works.

Self-assessment and the scoring matrix
During self-assessment, contractors are expected to rate themselves based on the implementation of each of the 110 NIST (SP) 800-171 cybersecurity controls. The CMMC requires DOD contractors to conduct these self-assessments once every three years unless anything necessitates a change. Because contractors are subject to DOD and prime contractor audits at any time, it's critical to maintain cybersecurity controls and have recent documentation validating that everything has remained secure and compliant.

The assessment scoring begins with a perfect score of 110 for each NIST 800-171 control. Points are then subtracted for non-implementation of controls. Each control holds a weighted point value ranging from one to five based on its significance.

No credit is given for partially implemented controls, except for multifactor authentication and FIPS-validated encryption. Although NIST does not prioritize security requirements, it declares that some controls bear a higher impact on a network's security.

Here are **four** things you must remember when it comes to self-assessment:

- If you don't receive a perfect score of 110 points, you must create a Plan of Action and Milestones (POA&M) document outlining how the deficiencies will be addressed and the failing items remediated. You can update your score when the shortcomings are addressed and remediated.
- As a contractor, you must also develop a System Security Plan (SSP) detailing implemented NIST 800-171 controls, such as operational procedures, organizational policies and technical components.
- Neither SSPs nor POA&Ms are uploaded to the federal database but must be available for audit.
- Upon concluding a self-assessment, you must submit your score to the governmental SPRS database within 30 days.

Now that we've established everything you must do, there's no time to waste. Let's talk about how we can help.

Get assessment-ready now!
To qualify for new contracts and renewals while CMMC is being rolled out, you must start gearing up to conduct a thorough and accurate self-assessment and do whatever it takes to fulfill today's cybersecurity requirements. This way, you will comply with the Interim DFARS Rule and be prepared for every future development with respect to CMMC.

Navigating through the complexities of CMMC can be both complex and overwhelming. That's why having an experienced partner like us can help ease the pressure. Contact us today to get our security experts in your corner.