RESOURCE CENTER

Become a cybersecurity MVP: The NFL and CISA on defying cybersecurity challenges

Get the full interactive view at https://bitwarden.com/resources/become-a-cybersecurity-mvp-nfl-and-cisa/

bitwarden

Tomás Maldonado, CISO at the National Football League, and Jeff Greene, executive assistant director of the cybersecurity division at Cybersecurity and Infrastructure Security Agency (CISA), joined Bitwarden CEO Michael Crandell for a fireside chat at the Open Source Security Summit to delve into security best practices, common mistakes and the breadth of resources available to organizations. They also discussed how individuals and organizations can outsmart cyber-criminals through frequent software patches, awareness of social engineering schemes, and using security tools such as multi-factor authentication and password managers.

After spending years as a security professional at high-profile financial firms, Maldonado held a CISO role at a chemical manufacturing firm and has experience working for highly regulated companies. Joked Maldonado, "The NFL put me through a cybersecurity combine."

At CISA, Greene and his team are responsible for cybersecurity, reducing cyber threats, and, ultimately, cyber attacks at the federal, civilian, and executive levels. While each agency has its own CISO, CISA sets policy and has the authority to give directives. Greene, who has 15 years of cybersecurity experience, was previously a lawyer. Before transitioning to his current role, he held roles in the private sector and with the National Institute of Standards and Technology (NIST).

Table of Contents

Understanding cyber threats

Understanding the nature and scope of cyber threats is crucial in the ever-evolving landscape of cybersecurity. Cybercriminals are constantly refining their tactics, making it imperative for security teams to stay one step ahead. New vulnerabilities and perennial issues like phishing and ransomware remain significant challenges as new technologies emerge.

Cyber threats come in various forms, each posing unique risks. Malware, for instance, is a formidable adversary, with attacks becoming increasingly sophisticated and stealthy. This category includes viruses, worms, ransomware, and cryptojacking, all of which can wreak havoc on systems and data.

Phishing attacks are another persistent threat targeting organizations of all sizes. These attacks often involve deceptive emails or messages that trick recipients into revealing sensitive information. Education, awareness, and robust security measures that detect and block these attempts are key to combating phishing.

Ransomware, a type of malware that encrypts data and demands payment for its release, is a significant concern. Organizations must be vigilant and employ comprehensive security protocols to prevent such attacks and mitigate their impact.

Preparing for these different types of cyber threats is essential for identifying potential attack vectors and organizing effective mitigation strategies. By understanding these threats and implementing proactive security measures, organizations can better protect their networks, systems, and sensitive data from cyber attacks.

Read more:

What is a cyberattack and how to stay secure

How the NFL and CISA identify cyber threats and collaborate on cybersecurity challenges

For years, the NFL and CISA have met 12-18 months before the Super Bowl. With the 2025 Super Bowl set to take place in New Orleans, the NFL has ensured that businesses offering services during the Super Bowl understand CISA's services, such as tabletop exercises, training, awareness campaigns, vulnerability scanning, and penetration testing.

The NFL and CISA also collaborate to identify and mitigate advanced persistent threats and sophisticated, prolonged cyberattacks that aim to steal sensitive information or sabotage operations. Cloud computing introduces unique cybersecurity challenges, making it crucial to secure cloud infrastructure against misconfigurations and inadequate access controls.

For example, a donut shop near the Super Bowl might take advantage of tools such as a public scan of the shop's public-facing websites, to ensure there are no vulnerabilities open to exploitation. CISA can also offer baseline security goals that will give organizations ideas on improving their security.

CISA has cybersecurity advisors in every state who can engage with businesses that face potential threats. While the type of threat an energy company may face is likely more severe than that of a donut shop, even a donut shop is likely to handle large amounts of personal information and can benefit from vulnerability scans. CISA is also heavily focused on helping businesses prevent and triage ransomware attacks. Said Greene, "If we believe a business is under attack right now or being targeted, we'll reach out directly and recommend counter-cyberattack measures they should be focusing on."

Password managers help safeguard against ransomware by enabling users to generate strong and unique passwords for each site they visit. This reduces the risk of password reuse and stops people from defaulting to weaker passwords simply because they're easy to remember, reducing the likelihood of credential theft.

Cybersecurity challenges when managing sensitive data

Businesses that operate as an "organization of organizations" face many unique cybersecurity challenges. The NFL oversees 32 clubs, each operating its own additional lines of business.

"The security practices, protocols, and programs we've designed are aligned with NIST cybersecurity recommendations. Of course, we also ensure we're taking advantage of the services offered by CISA. The individual clubs understand how the league can help them and also how they can locally benefit from government cybersecurity services." ~ Tomás Maldonado

Individual clubs often work closely with local businesses and services, and they pass on the security best practices they observe to their supply chain providers.

Read more:

Why enterprises need a password manager

Preventing cyber attacks through constant collaboration

Preventing cyber attacks requires a comprehensive approach to mitigate risks and protect sensitive data. Companies must invest in solutions that safeguard their systems from both internal and external threats.

Password managers can help users generate and store complex passwords securely. Encouraging strong, unique passwords and cultivating a culture of cybersecurity can prevent cybercriminals from gaining access to systems and arm employees with the tools and resources to identify and escalate potential threats. Implementing multifactor authentication (2FA) adds an extra layer of security by requiring users to provide two forms of identification before accessing systems, reducing the risk of unauthorized access, even if passwords are compromised. Encrypting sensitive data ensures that it cannot be read without the decryption key, even if it is intercepted. Setting up alerts for suspicious or malicious activity allows security teams to respond quickly to potential threats. By investing in these solutions and adopting best practices, companies can effectively respond to cyber attacks and protect their sensitive data from being compromised.

“In the years since [SolarWinds], we’ve made incredible progress in deploying endpoint detection and response at 60+ federal agencies. Now, we can analyze cyber threats and connect those proverbial dots across agencies. We have been able to use our resources to detect malicious activity that evaded our endpoint detection technologies because when we put it all together, we realized something wasn’t right. We were able to stop what we consider some next-generation attacks.” ~ Jeff Greene

Mitigating human error, insider cyber threats

Pivoting from corporate security and the opportunities and challenges present, Crandell pointed out that despite our sophisticated security technologies, human error remains one of the top causes of breaches. He asked Maldonado and Greene about strategies and practices that can be adopted to encourage better behavior.

“I try to drive awareness and education with my team about the types of threats we’re facing as an organization,” said Maldonado. “I also focus on security threats that people may face in their personal lives. While people may like to view their staff as the weakest link, I look at it through the lens of our staff being our greatest asset. If I have 15,000 people in my organization, I potentially have 15,000 security evangelists.”

“If I can reach them and make them more educated in cybersecurity, they may be good canaries or evangelists for certain security controls … Ultimately, people are well-intentioned and want to do the right thing.” ~ Tomás Maldonado

Maldonado also noted that people still rely heavily on usernames and passwords. He said the NFL has tried to shift from passwords to passphrases because he believes this will make it more challenging for adversaries to crack while simultaneously making it easier for individuals to remember.

Bitwarden users looking for an alternative to passwords made from randomly generated characters may also benefit from passphrases. Passphrases can be created using the Bitwarden Passphrase Generator or the item creation pop-up within the vault.

Prioritizing security by design

"If you teach people how to protect their personal information, whether it be credit card details or bank account data, they will transfer those skills - almost automatically - to their professional life," said Greene. "But, all of this focuses on the short-term problem, and there is a longer-term fundamental problem … We should not be living in an environment where a momentary mistake can lead to a cyber-criminal emptying a bank account, stealing national security secrets, or taking down critical infrastructure. That's happening because the software and technology we rely on are built insecurely."

"In the short term, we need to do everything we've discussed, and in the long term, we need to change how this technology is built. We need it to be rock-solid from the front end. We need security-by-design." ~ Jeff Greene

Examples of security by design include:

- Using multi-factor authentication.
- Reporting known vulnerabilities.
- Having a system to detect vulnerabilities.
- Ensuring no device or system comes with a default username and password.

Organizations should immediately change default usernames and passwords to strong and unique passwords or passphrases, preferably managed and secured by an encrypted end-to-end password manager like Bitwarden.

Greene also encourages everyone to check out the CISA website for more information on the official Secure by Design pledge.

Check out the official Secure by Design pledge.

The evolving security threat landscape, ransomware attacks, and success stories

As cyber threats continue to evolve and become more sophisticated, the role of AI and machine learning in cybersecurity is becoming increasingly important. It is critical that businesses adopt technologies that can detect and respond to cyber threats in real time, significantly reducing the risk of data breaches and other cyber attacks. With real-time threat detection, AI and machine learning algorithms can quickly analyze vast amounts of data, identifying patterns and anomalies that may indicate a cyber threat. By analyzing historical data, AI can predict future cyber threats and help organizations prepare for potential attacks.

"As AI becomes more mainstream, security practitioners need to understand better the potential security risks posed by generative AI and how we can implement secure-by-design principles to lay a strong foundation for data security," said Maldonado. He believes security by design principles must be integrated early as future developers learn to write code. "There's an incentive for developers to learn how to code very quickly so they can release a product to the marketplace as fast as possible," said Maldonado.

“We need to shift from a mindset of rewarding companies that release products quickly to rewarding companies that thoughtfully prioritize and build in security from the onset. It is possible for businesses to hit their market goals while protecting users from having their data compromised.” ~ Tomás Maldonado

This proactive approach allows security teams to stay ahead of cybercriminals and mitigate risks before they materialize. AI-driven systems can automatically respond to detected threats, neutralizing them before they cause significant damage. This reduces the burden on security teams and ensures a swift and effective response to cyber attacks. By leveraging AI and machine learning, organizations can enhance their cybersecurity posture and better protect their data from emerging threats.

“We are all empowered to improve the security of our digital lives and companies. As scary as it seems, most cyberattacks are not sophisticated, and most attackers are lazy. If you, as an individual or a small business, do the simple things - patch updates, have security tools such as password managers installed, and utilize multi-factor authentication - you will be ahead of most cyber-criminals.” ~ Jeff Greene

Get started with Bitwarden

Ready to become a cybersecurity MVP with password management? Get started with a 7-day free business trial, or sign up for a free individual account.

Check out this free eBook, Balancing Security and Innovation in the Age of AI, to learn about the threats generative AI can pose to your data and if your IT team is prepared.