protiviti®
Face the Future with Confidence

National Terrorism Advisory System (NTAS) Issues Bulletin on Potential Terrorism Threat to the U.S. Homeland From Nation-State Cyberattacks

January 7,
2020

On January 4, 2020, the Department of Homeland Security (DHS) issued a National Terrorism Advisory System (NTAS) bulletin describing current developments and general trends regarding the terrorist threat posed by nation-state cyber warfare programs. According to the NTAS, the catalyst for the bulletin's issuance is the United States' "lethal strike in Iraq killing Iranian IRGC-Quds Force commander Qassem Soleimani" and publicly stated intentions of "Iranian leadership and several affiliated violent extremist organizations … to retaliate against the United States." The bulletin is available at www.us-cert.gov/ncas/current-activity/2020/01/04/dhs-releases-ntas-bulletin.

It is important to note that while the bulletin specifically states that the NTAS has no information indicating a specific, credible threat at this time, it acknowledges that "an attack in the homeland may come with little or no warning." The NTAS also acknowledges that Iran has been implicated in previous U.S.-based plots and has the capabilities within its cyber program to carry out attacks against critical U.S. infrastructure. Accordingly, vigilance is the order of the day.

The Focus on Nation-State Cyber Threats Is Not New

If U.S. companies were attacked on the cyber front by a nation state, it would not be the first time it has happened. And the present threat is real – from several countries. Following are examples:

- On February 26, 2015, then Director of National Intelligence, James Clapper, testified before the Senate Armed Services Committee that the destructive cyberattacks during February 2014 was the first time such attacks were carried out on U.S. soil by nation-state entities, and were marked first by an attack against the Las Vegas Sands Casino Corporation.

- On June 22, 2019, the Cybersecurity and Infrastructure Security Agency (CISA) issued a Statement on Cybersecurity Threats citing the recent rise in malicious cyber activity directed at U.S. industries and government agencies. They further noted the use of "wiper" attacks with the potential to take down entire networks.

- In November 2019, a Microsoft security researcher presented findings at CyberwarCon from their threat intelligence group regarding malicious attempts to gain access to the networks of Industrial Control System (ICS) suppliers, which is a possible first step in a supply chain attack that could be used for acts of sabotage.

What Should Companies Do?

Protiviti recommends organizations take the following key actions to deter, identify and respond to a cyberattack. Given the source and nature of the threat, those business services that are defined as critical infrastructure sectors, or which otherwise have the potential to broadly impact many customers and stakeholders, should be prioritized when considering these actions.[1]

1. **Enhance security awareness.** One of the easiest ways to increase security is through employee awareness. Organizations should continue ongoing efforts to keep employees engaged and motivated, and, in view of the present threat environment, turn up the volume in their communications on this issue. In addition, they should:
    - **Increase awareness through testing for sophisticated phishing attacks.** Sophisticated phishing and spear-phishing techniques continue to defeat some of the best defenses. The technical perimeter is only as good as the human perimeter.
    - **Ensure the organization has updated information on indicators of compromise (IoCs) for recent attacks.** Such IoCs may include strange inbound/outbound network patterns, unexplained configuration changes, anomalous spikes in read volumes in certain files, log in red flags, unusual privileged user account activity and the presence of unknown files, applications and processes in the system.
2. **Identify the most critical systems, applications, infrastructure and third party needs to support important business services.** Organizations cannot maintain and build resilience in the face of significant cyberthreats, particularly those perpetrated by nation states, unless they have a clear understanding of their environment and the most important elements that enable the business to function.
3. **Implement mitigating controls to protect those critical technologies that cannot be patched.** These technologies may include medical devices, industrial

[1] For more about these sectors, go to www.dhs.gov/cisa/critical-infrastructure-sectors.

control systems and legacy applications, such as network segmentation and other solutions.

4. **Evaluate all access into systems and networks to ensure only authorized users can use or administer company assets.** To that end, it is vital to ensure that default credentials are updated.
5. **Increase the sophistication of protection and detection strategies.** One key step in the protection of systems and data is to increase monitoring of security events on systems with access to the internet. In addition, deploying more sophisticated defenses such as multifactor authentication (MFA) and active defense technologies (e.g., endpoint detection and response [EDR] and intrusion prevention systems [IPS]) can help mitigate risk to the environment.
6. **Seek and share the latest cyberthreat information.** Sharing of cyberthreat information among businesses, as well as between government and business, could help mitigate attacks from nation-states. There are numerous Information Sharing and Analysis Centers (ISACs) that can assist with the sharing process. Companies should connect with the appropriate ISAC to ensure they have the latest information. Those who are in possession of U.S. government data may prefer to access the Defense Industrial Base, or DIB, which aims to protect sensitive, unclassified Defense Department program and technology information residing on, or transiting among, Department of Defense and defense contractor computers. It makes sense to be informed.
7. **Refresh the risk assessment process as it relates to cyberthreats more than once a year.** Because threats are evolving so quickly, the risk assessment should be performed quarterly to ascertain the emergence of new threats and risks. In addition, the risk assessment process should consider risks beyond the loss of sensitive data. Other risks, such as operational impacts and disruption, could be realized through cyberattacks. Accordingly, it behooves companies to focus on designing appropriate cyber defenses to mitigate these risks as they emerge. The recent threat triggering the release of the NTAS bulletin is yet another reminder of the dangers lurking from sophisticated advanced persistent threats (APTs) perpetrated by nation states playing for keeps.
8. **Ensure the organization has a sound, up-to-date incident response plan that addresses new threats.** Conduct training and rehearsals of this plan through simulations (e.g., tabletop exercises). Revisit the plan more than once a year – ideally, quarterly – depending on the risks to the organization. Review organizational business continuity and disaster recovery plans and ensure they are up to date and include

recovery procedures for business disruption from a cyberattack, particularly for systems that are critical to the execution of the business model.

9. **Ensure cyber defenses are adequately funded and staffed to manage the evolving risks and threats.** An effective and comprehensive understanding of the threat landscape, including APTs perpetrated by nation states or state-sponsored groups, facilitates the allocation of defense spend to its highest and best use.

Concluding Thoughts

In issuing the NTAS bulletin, DHS indicated that it intends to provide protective measures when and if the understanding of the risk landscape changes. That said, it is up to each organization to take the necessary steps to protect its critical systems, assets and intellectual property and sustain its business model. The nine key actions we outline above offer a framework for assessing next steps near term.

How Can Protiviti Help?

Protiviti can assist companies in a variety of ways: Our professionals can:

- **Evaluate your cybersecurity program with a *rapid assessment*.** This one- or two-week project will examine your company's protection capabilities, abilities to detect cyber-related events, and incident response capabilities. The assessment also includes a tabletop exercise with executives, and the results will highlight areas of strength and weakness within your organization's cybersecurity program.

- **Implement and manage new cyber capabilities and technologies.** Cyberattacks are inevitable, and cyber technologies are transforming in parallel. With a growing need to automate, orchestrate and mature your organization's cyber capabilities, Protiviti can help you leverage technology (such as artificial intelligence and machine learning) to realize your efficiency in cybersecurity and grow securely.

- **Assess your risks and build your operational resilience program.** We use quantitative data-driven and evidence-based methods to define, scope, size and prioritize your cyber risks, to help you make informed business decisions and design a program that drives continuous improvement.

- **Find and train the right resources and skills to complement your team.** In partnership with Protiviti's parent company, Robert Half International, we will bring in the right people with the right skill set at the right time, based on your company's customized needs.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60% of *Fortune* 1000® and 35% of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Contacts

Ron Lefferts
Managing Director, Global Leader, Technology Consulting
+1.212.603.8317
ron.lefferts@protiviti.com

Curt Dalton
Managing Director, Global Leader, Security & Privacy
+1.617.330.4801
curt.dalton@protiviti.com

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.