GLOBAL GUARDIAN

STRENGTHENING CYBER SECURITY DURING COVID-19

GLOBALGUARDIAN.COM 703.566.9463 OPERATIONSCENTER@GLOBALGUARDIAN.COM

Strengthening Cyber Security During COVID-19

October is Cyber Security Awareness Month, which aims to raise awareness about the importance of cyber security across our nation. Even prior to COVID-19, cyber security has been one of the most pressing challenges facing companies. According to Cyber Security Ventures, an industry research company, cybercrime is expected to cost as much as $6 trillion annually worldwide by 2021. Ever since the COVID-19 pandemic began, Global Guardian has monitored developments on how the crisis is impacting cyber security to inform our clients and to expand our product offerings to meet our clients' changing needs. Recently released surveys of private enterprises provide us with a much fuller picture of how cybercriminals are exploiting the crisis and how organizations and individuals can best protect themselves.

With the unprecedented mass and rapid move to remote work and school during COVID-19, businesses and individuals are facing even greater barriers to securing their networks and maintaining business continuity. According to the cloud computing company iomart, the number of large-scale data breaches increased by 273% in the first quarter of 2020 compared to the same time last year. The FBI estimates that calls to its Internet Crime Complaint Center (IC3) rose as much as four-fold since the pandemic started. By late April, IC3 reviewed more than 3,600 complaints related to COVID-19 scams alone.

COMMON CYBERATTACKS AND THEIR ENTRY POINTS

Remote workers lack protection in the home that they have in the office. Often, their home internet infrastructure, such as modems and routers, are unprotected. This leaves them more susceptible to opportunistic cyberattacks that can be brought back to the office when they connect. Additional risks come from the many additional individuals outside of one's employees—from their spouses to their children—who may be sharing internet networks and (knowingly or not) the organization's electronic devices. According to the World Economic Forum's COVID-19 Risks Outlook, 50 percent of enterprises surveyed were concerned about increased cyberattacks due to the shift to remote. We are already seeing how cybercriminals are upping old tactics, deploying new ones, and exploiting fears about the ongoing public health crisis.

GLOBAL GUARDIAN CASE STUDY: UNPROTECTED INFRASTRUCTURE

When a partner at a wealth management company was hacked through her home wireless router in California, $82,000 was stolen from her bank account in just two months. Global Guardian was hired to evaluate and recover the breach. As a result, subsequent hacker attempts on her home network have been unsuccessful.

While there are a wide range of cyber security threats you need to be aware of, at Global Guardian, we advise our clients to pay close attention to:

- **Attacks on smart home automation systems such as Nest and Ring.** These systems are set up using Windows or Linux and require regular updates, including to fix mistakes in the original code. When these updates are ignored, hackers use network and vulnerability scanners to identify these instances to gain access. Once in, hackers can do everything from open your house doors to listen to your conversations.

- **Malware attacks**, which occur when attackers install malicious software on your device without your knowledge to gain access to personal information or to damage the device, usually for financial gain. In a March 2020 global survey by the software company VMware, 92 percent of enterprises reported an increase in malware attacks compared to before COVID-19.

- **Ransomware attacks**, which is a type of malware that extorts its victims by threatening to block access to specific files or an entire system or drive, potentially crippling the day-to-day operations of an organization. Unlike older and less advanced malware, ransomware is able to target critical business systems, which can do more damage to an organization, making it possible to extort higher ransoms and devastate operations. These attacks are disruptive, shake customer trust, and can be extremely costly.

GLOBAL GUARDIAN CASE STUDY: RANSOMWARE

Ransomware can be targeted or luck of the draw. And just because your company or home has been attacked once, does not mean the hackers will not attempt again. Nothing is off-limits to a determined attacker. Following a major ransomware attack, Global Guardian helped an American company fend off persistent attackers. Within 30 days the company was reattacked unsuccessfully several times by hackers. One of these attacks occurred the night of the holiday party at the CEO's home and was preceded by an attempted hack on the company earlier that day. For the next six months, Global Guardian monitored the network 24/7, defending against escalations of attack types.

- **Credential stuffing**, which involves hackers breaking into e-commerce, entertainment, or news sites and stealing usernames and passwords. Using stolen information from one credit or other account, hackers then test it in others to find out if they work. With many people stuck at home and spending time playing video games for entertainment, gamers have become an especially attractive target for credential stuffing. According to a report by Akamai, a content delivery network services provider, there have been 10 billion credential stuffing attacks targeting the gaming industry from July 2018 to June 2020.

- **Phishing attacks** in the form of malicious emails from hackers posing as legitimate COVID-19 updates from government and industry representatives or fundraising drives by charities to help those impacted by the crisis. The purpose of these phishing attacks is to trick users to disclose their email credentials, download attachments containing malware, or direct users to illicit websites.

ESSENTIAL CYBER SECURITY PRECAUTIONS

To protect your organization and your family, Global Guardian recommends adopting simple precautions such as virtual private networking, next-generation firewalls, and managed cyber hygiene, which can offset risks of workers operating remotely.

Corporate policies should require virtual private network (VPN) use for all remote work, including work performed on mobile devices. In addition, Global Guardian recommends the following:

- Ensure employees know how to connect to the VPN and understand the importance of a VPN

- Require the use of multi-factor authentication (MFA) where possible.

- Companies should use a reference framework to harden computers, keep patches up to date, and run vulnerability scans on any computer or mobile being used to connect through the VPN. In addition, they should ensure anti-virus software is installed, computer firewalls are enabled, and they are able to locate, remotely manage, or wipe employee devices.

It is important to remember that all the devices used to work from home will make their way back to the office and will be plugged in to the network, potentially introducing whatever malware was picked up while outside of the protected network.

This is a time of financial uncertainty for many companies, but cyber security must remain a priority. According to McKinsey & Company, "70 percent of the CISOs [Chief Information Security Officers] and security buyers believe budgets will shrink by the end of 2020 but plan to ask for significant increases in 2021." Business leaders should prioritize investing in the following as they evaluate their cyber security budgets:

- An assessment of your organization's digital infrastructure.
- Regular in-person or online cyber security trainings for the entire staff on how to stay protected inside and outside the office, including while traveling.
- A dedicated in-house CISO or an external Virtual Chief Information Security Officer (vCISO) consultant.

HOW GLOBAL GUARDIAN STRENGTHENS CYBER SECURITY

By planning and investing in cyber security in 2020, businesses can help better protect themselves against increasingly sophisticated cyberattacks to ensure business continuity.

Global Guardian's cyber security offering is designed to keep both corporations and individuals ahead of cyber threats and malicious actors. Our service offering includes expert baseline assessments, unparalleled real-time network monitoring, and analysis with a focus on the end user. In addition, if you are looking for maximal VPN protection, we recommend Global Guardian's VPN services for corporate, residential, and personal devices. Unlike other premium VPNs, Global Guardian's VPN service utilizes our custom threat intelligence feed to actively monitor your VPN tunnel for malicious activity.

Many businesses do not have a dedicated in-house CISO or may need additional support to manage cyber security effectively, provide real-time intelligence and make sure that software updates are properly installed and strictly monitored. Global Guardian's Cyber Security Concierge Service is designed to do just that. With 24/7 monitoring capabilities backed by a dedicated cyber team at the Security Operations Center, your requests are triaged by our cyber security analyst concierge and when required, your dedicated vCISO.

Global Guardian's VPN in conjunction with our tailored cyber security solutions provides our clients with the ultimate defense against today's cyber threats.

To learn more about how Global Guardian can protect your organization and family, contact our 24/7 Operations Center at operationscenter@globalguardian.com or + 1 (703) 566-9463.

GLOBAL GUARDIAN

CONTACT US

Please contact the 24/7 Global Guardian Operations Center at any time with questions or comments on this special report, or for any cyber security need.

OPERATIONSCENTER@GLOBALGUARDIAN.COM

+1 703 566 9463