WRITTEN STATEMENT FOR THE RECORD

OF

JOHN ZANNI
CHIEF EXECUTIVE OFFICER
ACRONIS SCS

BEFORE THE

US SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

SUBCOMMITTEE ON REGULATORY AFFAIRS AND FEDERAL MANAGEMENT

ON

“MODERNIZING TELEWORK: REVIEW OF PRIVATE SECTOR TELEWORK POLICIES DURING THE COVID-19 PANDEMIC”

Tuesday, July 28, 2020

Introduction

Chairman Lankford, Ranking Member Sinema, members of the Committee, it is an honor to join you today. Ranking Member Sinema, thank you for the invitation to come discuss the particular challenges associated with telework, in light of the ongoing COVID-19 pandemic.

Both of you have been instrumental in the Committee's efforts to educate the American people on the Nation's cybersecurity vulnerabilities and have developed bipartisan legislative initiatives that help address them—bills like your *Telework for U.S. Innovation Act* and the *Emergency Telework Act* before it.

With this in mind, I appreciate the opportunity to share my insight—informed by more than two and half decades in the cybersecurity field, including in my current role as Chief Executive Officer of Acronis SCS, an Arizona-based company dedicated to meeting the unique cyber protection and edge data security needs of the US public sector, including federal, state and local government, education, public healthcare, and nonprofit institutions.

Pre-COVID-19 Context

There is no question: the modern cyber threat landscape is more sophisticated and relentless than ever before. While COVID-19 has brought certain cybersecurity challenges into stark focus, like those associated with 2020's dramatic rise in telework, many of the threats we see reflected in headlines today are not new.

In 2019, for example, nearly one thousand US public sector organizations, including government agencies, education institutions, and healthcare providers, were hit with ransomware attacks, costing upwards of $7.5 billion – and those are just the publicly reported numbers.[1] In total, North America experienced 18,648 cyber incidents in 2019, including almost a thousand data breaches that compromised confidential information.[2]

Put simply, we had an epidemic of a different sort on our hands long before COVID-19, which has now become much more apparent and urgent.

Understanding Telework Vulnerabilities

The current pandemic has driven a massive move to telework, along with an increased reliance on technology and data outside of controlled environments. With that shift has come a staggering jump in criminal cyber activity from bad actors eager to take advantage of COVID-19 for their own personal, monetary, or geopolitical gain. The fear and confusion of the pandemic presented an opening, in the form of hunger for new information, that has made scams and phishing attempts more successful. To put data to the problem, the number of domains with "corona" or

[1] https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/
[2] https://enterprise.verizon.com/resources/reports/dbir/

"covid" in their names jumped from 190 in 2019 to more than 38,000 in March of this year.[3] Some of those websites are legitimate. The vast majority are not.

Since March, we have also seen a jump in scam emails purporting to offer safety tips from seemingly trustworthy sources, like the World Health Organization and US Centers for Disease Control. Once opened, malicious attachments and links introduce ransomware or other attack vectors that can spread throughout an entire network, presenting particular challenges for businesses and public sector organizations trying to keep critical services up-and-running.

The rapid shift to telework in response to the spread of the virus only amplified these and other cyber vulnerabilities. Virtually overnight, employees had to not only stay productive in an entirely new work cadence, but also protect sensitive organizational systems and data while far from the office. IT teams, in turn, scrambled to enable safe and secure telework capabilities, like adding virtual private network (VPN) lines and virtual desktops or deploying collaboration applications, like Microsoft Teams.

In both the private and public sectors, the dislocation between businesses operations and the workforces needed to sustain them that this pandemic has caused has both exacerbated existing cybersecurity vulnerabilities and created new ones. As your recent legislative initiatives recognize, the ability of businesses to survive the already daunting challenges presented by the pandemic will depend, in part, on their ability to adapt to a more mobile workforce with cybersecurity vulnerabilities in mind.

Today's typical home includes a spate of devices: desktops, laptops, tablets, smartphones and gaming consoles, some consumer Internet of Things (IoT) devices like smart TVs and home security systems, and maybe even a few network-connected toys and appliances. All these devices share access to a standard Wi-Fi router with basic security settings. The IT resources and processes we all take for granted in an office – regular patching of operating systems, software, network devices, and security appliances; network safeguards like firewalls and intrusion prevention systems; daily backups of all workloads; updates of endpoint anti-malware and firmware, and; help desk support – are often greatly reduced.

This environment is an obvious risk when employees use personal equipment to access an organization's private network, even with secure VPN connections, particularly when family members without proper security training share access to such devices. However, the home environment can also threaten the security of organization-owned devices, like a company laptop. Any device in the household (including unattended IoT devices) could inadvertently let in a piece of malware that threatens all connected devices, including those accessing the company or organizational network. Worse still, many IoT devices can never be patched for security vulnerabilities, leading to so-called 'forever-day' risks that make them particularly easy and appealing targets for cybercriminals.

The surge in use of videoconferencing and telecommunications applications – like Zoom, WebEx, and Microsoft Teams – has also presented new risks. The typical videoconferencing call

[3] https://intsights.com/resources/covid-19-cyber-threat-impact-report

involves multiple people connecting from home environments, some from personal devices over unsecured networks, into a single session. Without proper protections in place, such applications are vulnerable to message injection and code injection attacks, remote-control hijacking, watering-hole attacks via compromised third-party libraries and applications, session ID hijacking, exploits of outdated versions, man-in-the-middle attacks on chat and video streams, and redirection to malicious URLs.

As IT teams parse through these challenges, the risk of conducting business in such an environment is real. Last year, for example, even before we saw a steep incline in teleworking, thirty-nine percent of companies and fifty-six percent of public sector agencies reported suffering a major mobile or IoT-related compromise.[4]

In spite of such a complex threat landscape though, there is positive news as well: adopting a "defense in depth" approach to telework (and cyber hygiene in general), based on the concept of layered protection, will greatly diminish such risks. Simple tools and relatively easy-to-deploy processes, described in more detail below, are available to help organizations implement such an approach in their own environments.

A Successful Shift to Telework

As the CEO of a cyber protection and edge data security company, I had two primary priorities when the pandemic hit. The first was ensuring the safety of my employees, both physically and digitally, as we transitioned to a full telework posture starting in mid-March. The second was adjusting our processes to support customers in need of future-proof solutions that would help their own organizations stay safe not only during the pandemic, but long after.

Technical Enablement & Cybersecurity

I am fortunate that Acronis SCS was already well positioned for telework before the pandemic hit. All our employees had company laptops equipped with anti-virus/anti-malware protections, as well as a regular backup schedule. Acronis SCS also adheres to a strict zero trust framework, applied across the enterprise – from our office and data centers to our network, applications, endpoints, email, and cloud infrastructure. We leverage next-generation firewalls and segment our networks based on the least privilege access model. We also use a tool to prevent email-based malware incursions, as well as require multi-factor authentication (MFA) and certificate-based VPN for access to certain sensitive resources.

This layered "defense in depth" posture helped us easily shift to telework without disruptions or fear that an attack on one device would compromise the whole company. For example, each remote employee only has access to one company network rather than all. If their system is infiltrated, the impact will be narrowly contained.

[4] https://enterprise.verizon.com/resources/reports/mobile-security-index/

In addition to the processes and tools we already had in place, we pushed out new cybersecurity trainings to every employee and implemented an updated end user acceptable use policy, ensuring our staff clearly understood the security risks associated with telework and the precautionary measures they are expected to take to stay #CyberFit, like configuring at-home Wi-Fi routers for maximum security.

Every organization's security and usability needs are unique, but these tools and processes are easy places to start for an organization unsure of how to shore up cybersecurity in their own environment. For example, using a backup and disaster recovery tool that includes active anti-ransomware protection can safeguard your organization's telework endpoints from breaches, while an easy-to-use digital authentication solution can prevent bad actors from tampering with your data, no matter where it sits.

Physical Enablement

When we shifted to telework, my leadership team understood that technological tools and cybersecurity protocols were not the only ones needed to ensure success. Physical enablement has been key as well. At the beginning of the pandemic, our human resources team sent out a productivity survey to determine employee needs and concerns. From that survey, we discovered that several of our employees lacked the basic home office equipment needed to do their job, like desks, office chairs, and monitors. Many also lacked access to high speed broadband. In response, we provided every employee the opportunity to purchase necessary equipment for reimbursement and have included a monthly internet stipend in their paychecks, so they can upgrade to higher connectivity speeds.

Holistic Employee Support

My leadership team also recognized that the ability of our employees to stay healthy and productive requires a holistic approach. In order to ensure all staff stay up-to-date on the status of the pandemic and the resources available to them, we hold a bi-weekly company town hall where we discuss trends, highlight relevant resources and new federal legislation, and reiterate company goals.

To prioritize physical health, we made sure our company health insurance policy supports both telemedicine and emotional / mental health services. In addition to reminding employees of this access, we sent each household a special care package with masks, hand sanitizer, and disinfectant wipes.

For some of our employees, the sudden shift to telework meant they no longer had any human-to-human contact. To help alleviate that isolation and encourage continued company camaraderie, we host bi-weekly virtual social hours and activities.

On the other side of the spectrum, many of our employees now juggle working from home with significant others, children, and pets all vying for their attention. In response to that reality, we implemented a more flexible work schedule, which has helped boost productivity and reduce employee stress levels. We also send out weekly emails with links to virtual activities and resources for families stuck at home.

Productivity Factors

In addition to adopting more flexible hours, the company prioritized other productivity-enhancing measures as well. We updated our management objectives system to better outline and measure employee performance. With an eye towards resilience, we ensured every member of the team had a backup person well-versed in their job duties, in case someone got sick and had to take time off to recover.

We also made virtual engagement and impromptu meetings just as easily accessible to employees as they would be in office. For example, our sales and customer support teams keep a Zoom group chat open all day long, to facilitate collaboration and cross-team communication.

Continued Customer Focus

In addition to adopting new policies and practices to better support our employees, when the pandemic hit, we also doubled down on our commitment to provide software that meets the unique security and usability needs of US public sector entities, whether that be an agency keeping mission critical assets, like industrial control and weapons systems, up-and-running, or a municipality protecting new telework endpoints, like employee laptops and phones.

We have stayed up-to-date on the challenges our customers face as they adjust to remote work realities, such as adding hundreds of thousands of new VPN lines, deploying thousands of remote desktops, or even considering expanded bring-your-own-device (BYOD) policies for affordability reasons. We have also taken every opportunity available to help amplify understanding of vulnerabilities (like the risk of turning off VPN or MFA, for example) and educate our customers and the wider public on cybersecurity best practices.

We also released a new solution in April, Acronis SCS Cyber Protect Cloud, designed to help organizations address telework challenges. The offering combines reliable backup and disaster recovery, full-stack anti-malware protection, and endpoint security and management capabilities (like automatic patching, remote desktop, and Zoom security) in one easy-to-navigate management console.

Increased Urgency

The rise in telework has brought with it a spate of challenges – but it has also renewed urgency to better address those challenges with more future-proof approaches. I want to thank the Homeland Security and Governmental Affairs Committee for its efforts to bring cyber hygiene issues to the forefront of the legislature's priority list and Americans' minds.

In 2020 alone, this Committee has introduced six bills directly relating to cybersecurity and two more regarding federal telework policies. That level of urgency is absolutely critical. Ranking Member Sinema, as the leader of a Scottsdale-based company, I must also express my sincere thanks for your leadership to ensure Arizona is secure, including your co-sponsorship of the *Cybersecurity State Coordinator Act* earlier this year.

From the recommendations outlined in this year's Cyberspace Solarium Commission Report, several of which I am encouraged to see have been incorporated into NDAA amendments or introduced as bills, to the Department of Defense's much-needed Cybersecurity Maturation Model Certification (CMMC), all signs point to increased urgency and impactful change – and a more secure Nation and robust economy as a result.

This growing urgency on cybersecurity in general lays the groundwork for more future-proof responses to telework vulnerabilities in particular. This is not a private sector or public sector concern. As our society and institutions become more interconnected, a breach or attack on one will have reverberating impacts on all. Moving forward, as issues like unemployment and healthcare dominate discussions of the COVID-19 response, America cannot afford to relegate cybersecurity to the back-burner. The risks of doing so are simply too high.

A Practical Framework for Building Digital Resiliency

As the urgency to address critical vulnerabilities and policy gaps grows, our Nation's public and private sectors need a cyber hygiene framework that promotes long-term digital resilience over quick fixes.

With healthcare top of mind, we can use that industry's model to prevent and treat illnesses as inspiration for the type of dynamic cyber protection plan organizations of all shapes and sizes must adopt – a plan which considers the inevitability of attack and identifies what policies and practices are needed to quickly and effectively recover.

Prevention – Like vaccines that proactively prevent illness, cyber protection tools and processes like vulnerability assessment, patch management, regular backup schedules, continuous data protection, and a zero trust architecture are key for helping companies and government agencies maintain cyber hygiene across all endpoints and prevent critical downtime and data loss.

Detection – Similar to the testing that takes place in the medical field, IT teams must employ artificial intelligence (AI) based threat detection and behavioral analysis (like URL filtering) on all endpoints and systems, so abnormalities can be easily and quickly identified.

Response – Once an illness is discovered, doctors can administer medication in response. Similar steps must be taken when an attack, hardware failure, or human error occurs on the cyber front. IT teams should streamline the response process by employing automated alert and remediation tools that allow for real-time reactions and triage.

Recovery – When illnesses or injuries become serious, doctors may perform surgery to help a patient recover. Similarly, once a cyber incident occurs, IT teams must focus on quickly restoring systems and avoiding the devastating downtime and data loss that could spell disaster.

Forensics – After an illness or injury is discovered, the medical community conducts extensive research to better understand the ailment and what can be done to treat it more effectively moving forward. Such post-incident investigation and analysis are equally as critical in the cyber realm. After an attack or failure occurs (an inevitability for every institution, no matter how good its prevention methods are), IT teams and end users alike must understand the causes of the incident – and how to avoid something similar in the future.

Conclusion

Whether COVID-19 subsides next week or next year, it is clear that increased telework flexibility is in America's long-term future. In light of the threat landscape described above, there is little time to waste in building digital resiliency and strengthening cyber hygiene.

Far too often, commercial and government needs are placed at odds with one another when it comes to cybersecurity. That reality must change – but it will take more buy in and collaboration from all sides of the equation, including private companies, Congress, and federal, state, and local government agencies. On the private sector side, companies must make a more robust commitment to consider public sector needs when developing solutions to cyber challenges. My experience at the helm of Acronis SCS has taught me that doing so is not always the easiest or most profitable route, but it is the right one for ensuring our national security and prosperity.

To close, I would like to borrow a few of Ranking Member Sinema's words from April of last year: "The United States must do a better job of developing cybersecurity standards, educating users about the cyber risks and solutions for connected devices, and increasing transparency for consumers." I could not agree more – and both I and Acronis SCS stand ready to serve as committed partners in that effort.

Chairman Lankford, Ranking Member Sinema, members of the Committee, thank you again for the opportunity to be here today. I look forward to hearing your insights and addressing your questions.

###