Internet Security Alliance Response to DHS CISA on Cross-Sector Priorities and Needs During Coronavirus Pandemic

First 30 Days – Coronavirus Cyber Risk 1 (a & b)

UNPLANNED SHIFT TO REMOTE WORK CREATES MASSIVE NEW RISKS

Key Idea:

Prior to the virus, no more than 20% of employees worked remotely. In the last few weeks, that number has jumped to close to between 80-100% of the workforce now working remotely. This may be the fastest and most disruptive technological shift in global work conditions in history. Two immediate developments create unique cyber risks and must be addressed by CISA ASAP.

a. The "work-around" infrastructure itself is not secured appropriately.

Currently infrastructure is unable to scale to a full pandemic event, forcing people to seek alternatives away from corporate standards and security by using services such as Zoom and Google Docs for sharing, which may not have the enterprise-ready security controls present. These applications may be economically necessary to promote a viable working environment, but do not have the same level of security posture, access management, and data protection, and thus present a significant threat for data exfiltration. Further, insecure and unpatched employee PCs and mobile devices increase the likelihood of adversaries exploiting systems as the workforce works from home, and insecure connections can result in compromised data in transit. As the crisis wears on, the economic pressure to elevate functionality and efficiency over security will grow. Moreover, organizations that historically rely on "perimeter-based" security models are left even more exposed to malicious actors when the workforce adopts a fully distributed telemetry for working practices.

b. Managers in traditional environments are not trained or prepared to manage securely.

Due to the near-immediate switch to unplanned online business, most managers have no idea how to run their operations using remote workforce and online tools in a secure fashion. The federal government needs to provide immediate managerial best practices on a ubiquitous basis to contain the cyber risk from growing exponentially.

Remote work programs that normally would be designed, tested and implemented incrementally over an extended period are being operationalized for entire workforces of many companies with no period of planning or adjustment. Additionally, many businesses have non-existent or incomplete business continuity plans. While IT planning seems to be more technology-focused, it is even more critical that businesses begin planning for the people impacts (i.e., chain of command approvals, etc.) should

workers be lost due to the pandemic. The lack of robust continuity plans may also lead to employees adopting "shadow IT" (i.e., using unauthorized workarounds or programs in order to better do their jobs while potentially circumventing installed security measures), and inadvertent disclosure of information (including physical access to employee workspaces and logical access to employee home networks) become more likely.

The vast majority of managers are substantially unprepared to manage this transition and often don't have access to the consultative assistance they would normally rely upon. They need succinct, validated, expert guidance, and they need it quickly.

We are already seeing cybercriminals and nation-states taking advantage of these multiplied vulnerabilities, especially with respect to targeting often-untrained employees and supply chains for attack.

WHAT GOVERNMENT CAN DO

Risk A – Better secure the "work-around" infrastructure.

Key Idea: As organizations transition to a heavily remote workforce, there is a need for tools for industry to assess and respond to cyber risks related to their network exposure and supply chain. The private sector could be greatly supported by government-developed tools to help organizations get a better picture of their network exposure and supply chain risk. Government can support such moves either directly or through alignments with the private sector. Systems and tools initially designed for military operations, which assume mobile operations that need to be secured, may need to be aggressively "lent" or transitioned to the private sector. The government should facilitate the adoption of multifactor authentication, as it is the single most important control for all critical business systems such as e-mail, databases, OT/ICS systems, VPNs/remote access points, etc.

Risk B – Providing mangers from traditional environments with tools for securing their mobile employees.

Key Idea: Provide management with information about how to address security issues they are otherwise unprepared for.

Six weeks ago, DHS/CISA, in conjunction with the National Association of Corporate Directors (NACD), the Internet Security Alliance (ISA), and the U.S. Department of Justice (DOJ) released three "toolkits" at the RSA Conference specifically covering cyber incident response, supply chain risk management, and insider threats. DHS needs to get these basic tools out to all corporate managers.

The toolkits were developed though a year-long, multi-sector collaboration with NACD, ISA, DHS, and DOJ as part of an update of the NACD Cyber-Risk Oversight Handbook (available free of charge at the following websites):

http://isalliance.org/wp-content/uploads/2020/02/RD-3-2020_NACD_Cyber_Handbook__WEB_022020.pdf

https://www.nacdonline.org/insights/publications.cfm?ItemNumber=67298

The advice is succinct (10 pages cover the three areas) and process-oriented, and the techniques have been previously validated by PricewaterhouseCoopers in their Global Information Security Survey. The approaches laid out in the NACD Handbook in these areas are also promoted in NIST's draft guidance on enterprise-wide cyber risk management.[1]

Government should immediately use all available mechanisms – both government and private partnerships – to aggressively push out these already approved and endorsed techniques to as broad an industry population as possible.

These best practices will provide managers with an easy-to-follow, validated set of directions they can use as they begin to get their arms around the massive transitions they are managing and identify security gaps they may be able to quickly close simply through awareness of the techniques contained in the "toolkits," and thus help forestall future risk.

First 30 Days – Coronavirus Cyber Risk 2

CISA NEEDS TO LEAD IN DEVELOPING A MORE AGGRESSIVE APPROACH TO INFORMATION SHARING

Key Idea: In time of crisis, a more aggressive posture on the part of the federal government in terms of being willing to share information is required. CISA should lead the way in establishing this new attitude.

WHAT GOVERNMENT CAN DO

For decades, the private sector has maintained that information they receive from the government is not timely and is often already available to the public from ISACs or security-oriented news channels. Given these emergency conditions, more aggressive sharing by USG is required.

Government needs an attitudinal change regarding information sharing. There are multiple examples when government is learning of specific weaknesses but not promptly relaying this information. Examples include the "Zoom bombing" issue or specific threats by actors who are shifting to new TTPs to take advantage of the situation or the VPN attacks and website watering holes for those who are operating unfettered on the Internet.

The traditional USG attitude is to watch and learn and not to share for fear that they will give up a potentially discovered advantage; or they don't want to share because they need to leverage this new information from a prosecutorial position on a case they are working against an adversary.

Getting the USG to focus on those weaknesses for the next few months and very quickly increasing their volume, veracity, and velocity of information sharing will help all of us defend together and get through these unprecedented periods of time. CISA should lead the effort to break through the barriers in the USG bureaucracy that prevent timely information sharing by leveraging the crisis ("don't let a good crisis go to waste"), which can then hopefully become the new normal for higher-quality information sharing even after this is all behind us.

[1] *Integrating Cybersecurity and Enterprise Risk Management,* National Institute of Standards and Technology, pg. 30

This intelligence should be labeled as COVID-19 related, not just general intel and needs to be both strategic and tactical. Government should also share general guidelines for strategic intel, and intelligence should be divided into industry vertical and/or supply chain roles to allow for faster consumption. Finally, the intelligence needs to be easy to read and consume. Overly long alerts, transcripts, etc. just end up being ignored by most, and therefore it is key for government to provide quick and easily digestible intel.

First 30 Days – Coronavirus Cyber Risk 3

CYBER WEAKNESSES THAT AFFECT HEALTH CARE SUPPLY CHAIN

Key Idea: The healthcare sector is already under immense pressure with their core mission. This sector now needs additional assistance managing the cyber risks that their normal operations may miss.

Confusion related to the uniqueness of the newly dominant online environment, well-documented economic disparities on the critical healthcare marketplace, and urgency will lead to disruption and increased inefficiency in the healthcare supply chain. While the observed overall volume of malware being hosted on websites has gone down, the content of existing activities is concentrated on COVID-related themes. With growth in legitimate sites hosting COVID content, cybersecurity experts face challenges distinguishing legitimate sources and filtering out malware and ransomware from incoming traffic. Specifically, ransomware will continue to be a threat to all organizations. Adversaries will use phishing attacks and remote access points to conduct these attacks, as the pandemic has greatly increased the risk to organizations, as hackers retool their campaigns to exploit COVID-19 fears and IT teams reconfigure their networks for remote access. As a result, organizations will need to maintain updated phishing blacklists and implement secure remote access infrastructure (e.g., VPNs with multifactor authentication).

Additionally, more severe malware could become a problem. For example, Emotet (the most prolific malware seen across all industry sectors) can be used by hackers to download and deploy additional payloads (including those that exfiltrate data), encrypt files (i.e., ransomware), and even cause physical damage by overloading computation and network resources. This risk is a particular concern for manufacturers with OT and ICS systems during the pandemic.

This will exacerbate delays with COVID-19 testing, delays with getting necessary medical equipment and medicine, and with getting food and necessary supplies.

There is also the likelihood that the supply chain for computer hardware could be disrupted. For employees, this means many health care workers will have to rely on a “bring your own device” model, causing employees to work completely outside corporate constructs. As a result, organizations may need to have conversations about relying on personal devices as fallback devices if they are unable to procure new laptops in a timely manner for onboarding. Further, cloud service providers may not have access to replacement hardware if needed and may continue to see unplanned downsizing on computing capabilities. This could cause on-premises applications to have to be doubled on hardware or go away until new computing resources can be procured, further compromising treatment in an already chaotic and highly pressurized environment.

WHAT GOVERNMENT CAN DO

The federal government needs to aggressively push out current supply chain cyber intel and cyber guidance such as the NIST guidelines and those laid out in the NACD Handbook. For example, the NIST guidelines can guide larger organizations on conducting cyber-risk analysis to better understand supply chain threats[2]. The NACD Toolkit on Supply Chain and Third-Party Risks offers basic guidance on how to conduct third-party risk assessments, which are more accessible to smaller health care operations including: Initial and ongoing monitoring of third parties, assessment processes and identification and remediation of weaknesses and threats.[3] The federal government can improve the private sector's cybersecurity posture by pushing out tools that help organizations better understand supply chain risk and the corresponding impact/exposure. More specifics can be found at the citations listed in the footnotes.

Government can also support the private sector also by providing guidance on how to distinguish between legitimate COVID-19 sources and those being utilized by hackers to help organizations adjust to remote work while minimizing risk.

Specifically, for the health care supply chain, the government could offer a simple self-service tool that allows organizations to quickly understand their exposure related to each supplier with high-level recommendations. Due to the shift in the risk landscape, the government could support the private sector by offering a simple self-service tool that allows organizations to see how their exposure profile has changed from pre-COVID-10 to post-COVID-19 with guidance. Finally, to help protect the financials of the organization, government could offer revised guidance or tools to help organizations better understand risk transfer (like cyber insurance).

Government can also aid in addressing growing ransomware and other major cyber threats like Emotet by sharing insights into phishing domains and hacker infrastructure to allow organizations to better defend against attacks.

First 60 Days – Coronavirus Cyber Risk 1

WORKAROUNDS TO MAINTAIN ECONOMIC VIABILITY WILL LIKELY BE PREFERRED OVER SECURITY SO FUTURE FEDERAL STIMULUS FUNDING OUGHT TO BE TIED TO SECURITY

Key Idea: In an environment where the economy is crashing and there is tremendous societal pressure to keep it afloat, companies may feel compelled to reduce best practice security controls in order reduce friction and/or improve performance with their new heavily remote workforce, which will potentially lead to a loss and/or destruction of sensitive data.

Specifically, reducing security controls will increase insider threat concerns and will likely put pressure on existing or future enterprise security certifications such as ISO 27000/27001 and SOX. This issue is exacerbated along the supply chain as other companies that have your sensitive data in their possession may also reduce their security practices, potentially putting your data at risk.

---

[2] *Integrating Cybersecurity and Enterprise Risk Management,* National Institute of Standards and Technology, pg. 15

[3] *Cyber-Risk Oversight 2020 Handbook*, National Association of Corporate Directors, pg. 45

WHAT GOVERNMENT CAN DO

With the virus' significant impact to the economy, nearly all businesses are struggling from a reduced revenue plan for the year, which will eventually have an impact on information security budgets and spending. This will, in turn, slow down or postpone planned critical improvements in cybersecurity capability or maturity.

Thus, for economic reasons, security spending is likely to be negatively impacted by the virus at the same time that the attack surface has expanded dramatically through the expansive online work activity.

The need to create new market incentives to promote cybersecurity has never been clearer.

Following the multi-trillion-dollar emergency funding the government has already provided, we are very likely to see another extremely large government stimulus package. Unlike the emergency funding, which was largely universal in terms of its targets, the next stimulus package may be more appropriate for at least some targeting – cybersecurity ought to be one of the items that deserves targeted stimulus funding for all sectors in the next legislation.

This program will not only reduce risk by shoring up online practices but instill these practices so they may become standard operating procedures after the virus crisis ends.

A key component to incentivizing cybersecurity is helping enterprise leaders understand the cost and benefits of cybersecurity controls. To do this, we need economic metrics that lay out cybersecurity risk to the organization (and proposed controls to mitigate those risks) in financial terms. The Cyberspace Solarium Commission stresses scaling up security by partnering with the private sector and adjusting incentives to produce positive outcomes and recommends establishing a bureau to develop cyber economic metrics.[4] The government needs to do more to help businesses understand the economic benefits of implementing cybersecurity controls and to identify where gaps remain where it is not commercially viable to do so. These gaps are where government needs to step in and offer some sort of incentive to bolster private sector security to meet national security objectives. Government needs to begin identifying where these gaps exist in order to target where additional cybersecurity funding might be warranted in upcoming stimulus packages.

First 90 Days – Coronavirus Cyber Risk 1

Key Idea: Establishing new identities: Trusted identities, especially for cross-trust with the USG, typically require face-to-face proofing and vetting of credentials to establish an individual's physical identity in order to create a secure digital identity that can be used for accessing corporate and third-party applications and digital resources. This process is essential for onboarding new members to a company as well as approved non-employee access across your supply chain.

- Our adversaries understand this scenario very well, and using social engineering tactics to get false identifies established is a significant concern when there is no face-to-face validation of the proofing and vetting steps ensuring the person is whom they claim to be.

[4] Cyberspace Solarium Commission Report, pg. 4. These policy approaches are also supported in ISA's Cybersecurity Social Contract (pg. 7) and the NACD Cyber-Risk Oversight 2020 Handbook (pg. 53).

- The USG has this same problem within USG operations: Government needs to develop creative ways to validate pedigree and documentation (such as using video cameras and in-person vetting with glass and drawer separation) to continue identity management operations.

WHAT THE GOVERNMENT CAN DO

- The USG can help by quickly sharing discovered techniques and recommended countermeasures with the community so private sector organizations can widely adopt these practices.
- The USG can help by implementing video-based interviews for clearances versus face-to-face so that USG clearance processing may continue during this crisis.

First 90 Days – Coronavirus Cyber Risk 2

Key Idea: There will be increased probability of Systemic Cyber Risk (related to Aggregation Nodes).

The remote workforce places a greater dependency on outsourced service providers, and heavily distributed resources increase dependency on utilities and national core infrastructure that were most likely not previously considered. This could result in business disruption (from a single cyber incident with broad impact) with a wide range of results, including: Unavailable employees (10% or more) that directly impact production and unavailable critical servers and applications that directly impact production.

The primary systemic cyber threats in this regard include but are not limited to insider and privileged misuse, miscellaneous error, crimeware (including ransomware), denial of service attacks, and environmental.

WHAT GOVERNMENT CAN DO

Government needs to develop a response plan with an emphasis to improve vulnerabilities and allow for greater redundancy that is difficult under current regulation or capitalism. The federal government should commission a study that accesses modern economic analytic methodologies and existing data, such as in the insurance industry, to model systemic risk. This analysis will need to be sector by sector, and given current environment, the health care sector would be a likely place to start.