AN OFFERING FROM BDO'S CYBERSECURITY PRACTICE

BDO CYBER THREAT INSIGHTS

2018 4th Quarter Report

SPECIAL FOCUS:
THE CYBER THREATS TO THE PUBLIC SECTOR

BDO

In this issue

Preface

This year has proven to be a challenging one for cybersecurity professionals worldwide. We have seen the blurring of the major cyber threat actors—nation-state cyberattack groups from China, Russia, Iran and North Korea—with criminal cyberattack groups from their respective countries and other nations worldwide. As a result, there has been a 350 percent increase in ransomware attacks globally, a 70 percent increase in the number of spear-phishing email attacks and the unprecedented growth of Business Email Compromises (BEC), also known as spoofing campaigns. The cyberattack groups are continually modifying their attack vectors, methods and tactics to: (1) optimize theft of money, cryptocurrencies and intellectual property; (2) disrupt national economies, social media platforms and political campaigns; and (3) destroy valuable data assets on a global basis.

At BDO, we have significantly grown our Cybersecurity and Information Technology advisory resources and managed security services capabilities during 2018 to offer more valuable services to our clients worldwide. Today, we have a team of more than 2,500 cybersecurity and IT professionals in 31 countries on six continents, and they are all here to serve the needs of the public and private sectors in protecting their information assets.

During 2018, our BDO global cybersecurity threat intelligence team has developed and published quarterly cyber threat insight reports to inform and educate our partners and clients internationally about the evolving cyber threat landscape. In the first quarter of 2018, we focused on significant cyberattacks and cyber events globally. In the second quarter of 2018, we created a Cyber Threat Insights Report with a special focus on the global healthcare industry. In the third quarter of 2018, our Cyber Threat Insights Report focused on the global banking and financial services industry.

In this issue for the fourth quarter of 2018, we discuss major cyberattacks on the global public sector. Plus, we delve deeper into the national cybersecurity strategic plans of four countries: Australia, Germany, Israel and the United States, written by our BDO Cybersecurity team leaders in each respective country.

At BDO we have developed an approach to preparing for potential cyberattacks, which we call Threat-based Cybersecurity. Put simply, we believe each client is unique and should have a comprehensive understanding of the actual cyber threats facing their respective organization. Thus, we prefer to start each client engagement with a set of advanced cyber diagnostic assessments. And then, based on the findings of our advanced diagnostic assessments, we develop a customized cyber defense plan to address each client's specific cyber needs, timeline and budget.

As a result of the tremendously positive feedback we have received from our partners and clients about the quarterly 2018 BDO Cyber Threat Insights Reports, we're happy to announce that we plan to continue the series through 2019 and beyond.

All the best!

Sincerely,

GREGORY A. GARRETT, CISSP, CPCM, PMP
Head of U.S. & International Cybersecurity for BDO

Read more ▶

Global Public Sector - Challenges

The public sector, including both government agencies and government contractors, has historically been a prime target for cyberattacks. Over the last few years, we have seen an escalation in the number and severity of attacks, threats and malicious actors targeting the sector. To understand the risk and underlying issues affecting the public sector, we must understand that it is not homogeneous. The sector is by definition governed and budgeted by a single overarching civic body (the federal government), which encompasses all public services and enterprises. But despite this, each entity within the sector has different objectives, agendas, political restraints and a multitude of other factors that set it apart from other entities within the sector. For example, establishing a clear segmentation between the private and public sectors can be challenging because of numerous overlaps between the two. This is further complicated by the growing trend towards privatization. For this reason, the public sector contains civil governmental agencies, including state and local municipalities, and some critical infrastructure and services. Moreover, while much commentary focuses on the U.S. government public sector, many of the issues presented are applicable to governmental organizations around the world.

CURRENT BASELINE

Incidents and data from recent years support the undeniable conclusion that the public sector struggles on multiple levels with IT and cybersecurity. The U.S. Government Accountability Office (GAO) concluded in a report to the Congressional Committees dated September 2018 that urgent actions are needed to address the cybersecurity issues and challenges facing the U.S.[1] GAO outlines a number of salient concerns that must be addressed which could apply to almost any nation state:

IT Systems Supporting U.S. Federal Government Agencies and Critical Infrastructures are Inherently at Risk

As disruption to these systems can be highly damaging and even life-threatening, they are a prime target for both cybercriminal and nation-state actors. Further compounding the risk is that these systems are highly complex, technologically diverse and often geographically dispersed. Federal systems and networks are often interconnected with other internal and external systems and networks, including the Internet. This trend, which will only continue to grow with technological advancements, creates numerous opportunities and venues for attacks.

Sensitive Data, Including Personally Identifiable Information (PII), is Becoming Easier to Gather and Analyze

Advancements in technology, such as data analytics software and IoT products, have made it easier for individuals and organizations to gather, analyze and correlate data on a vast scale. This generates a problem that is two-fold. Firstly, such databases are targeted and abused by malicious actors; and secondly, malicious actors can weaponize seemingly innocent products such as smart watches.

To illustrate this point, in early August the Pentagon banned deployed service members from using wearable technology that relies on geolocation including fitness-tracking devices,[2] as they can expose the location of bases and other critical facilities.[3] This policy came into effect just three months after the Pentagon also enforced stricter rules regarding the use of mobile devices within the Pentagon and supported buildings.

[1] https://www.gao.gov/assets/700/694355.pdf

[2] https://www.militarytimes.com/news/your-military/2018/08/06/devices-and-apps-that-rely-on-geolocation-restricted-for-deployed-troops/

[3] https://www.militarytimes.com/news/your-military/2018/01/29/dod-reviewing-stravas-global-heat-map/

Read more ▶

Poor Information Security Practices Are Common

While poor security practices are well-documented, it appears that the public sector continuously struggles to mitigate them, as is poignantly outlined in a government-wide cybersecurity risk assessment report from the Office of Management and Budget (OMB) published in May 2018. The report, which was conducted in coordination with the Department of Homeland Security (DHS), looked to determine federal agencies' ability to identify, respond to and recover from cyber intrusions. It examined 96 federal agencies' performance across 76 metrics and found 71 agencies to be "At Risk" or "High Risk."

One of the most alarming points is that more than half of the agencies have a limited ability in discerning what software runs on their systems. As a result, they do not actively whitelist software; a critical practice when managing cybersecurity frameworks. Further, they often have multiple versions of the same software installed and/or several redundant tools with overlapping functionalities. This in turn exposes them to a host of problems, the most glaring of which might be the considerable hindrance to the identification and mitigation of vulnerabilities and threats. Additionally, this also impedes the investigation process of incidents. The limited situational awareness is so debilitating that federal agencies often cannot even identify the method or vector of attack.

Of the 30,899 incidents where data or systems were compromised in 2016, agencies failed to detect the attack vector in 38 percent. As stated in the report, governmental organizations simply lack the network visibility to effectively detect and respond to cybersecurity incidents, such as data exfiltration attempts. In recent years, government-wide initiatives and policies, such as Trusted Internet Connections[4] (TIC) and National Cybersecurity Protection System[5] (NCPS) programs have attempted to address some of these issues. But, despite being well-intentioned, results have shown that these programs resulted in ineffective security frameworks that hindered performance and impeded adoption of commercial technology.[6]

Aging Legacy Government Information Systems

Unlike many industries within the private sector, which are largely dictated by market demands and can be more flexible, the public sector is often encumbered by significant bureaucracy.[7] This is manifest, for example, by the need to comply with outdated systems and standards that can significantly differ from agency to agency, not to mention from country to country.

For instance, according to a 2013 research report by the UK Department for Business, Innovation & Skills, the number of standards relating to cybersecurity exceeded 1,000 publications globally that year.[8] This in turn creates a complex standards landscape that impacts both the IT operation within governmental organizations and cybersecurity services given to them from third-party providers.

In fact, the American Technology Council[9], which was created by the White House in 2017 with the purpose of modernizing government services, found several glaring problems when it reviewed this matter. Most notably, when individual agencies issue agency-specific IT contracts, they often stipulate so many limitations that outsourcing network and security services becomes significantly more expensive than it should be. [10]

The second issue is the inherent difficulty of replacing legacy systems. Beyond the high cost, a blanket re-platforming of core legacy systems is highly risky for several reasons[11]; not in the least are unpredictable costs and consequences. Processes and the ways in which legacy systems operate are often inextricably intertwined. If a legacy system is replaced, these processes also have to change with potentially unforeseen complications.

For example, in the UK, a recent attempt by TSB bank to upgrade its systems went awry.[12] Although this incident occurred in the private sector, it depicts risks that could occur in any system. In April 2018, TSB transferred its customers' accounts from Lloyds Bank systems to its new Proteo4UK core banking system. Customers began to experience serious problems with their mobile and Internet banking services. During the outage, customers were locked out of their accounts and saw money disappear from online accounts.

[4] https://www.dhs.gov/trusted-Internet-connections

[5] https://www.dhs.gov/national-cybersecurity-protection-system-ncps

[6] https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf

[7] https://www.forbes.com/sites/jodywestby/2015/06/15/the-government-shouldnt-be-lecturing-the-private-sector-on-cybersecurity/

[8] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/261681/bis-13-1294-uk-cybersecurity-standards-research-report.pdf

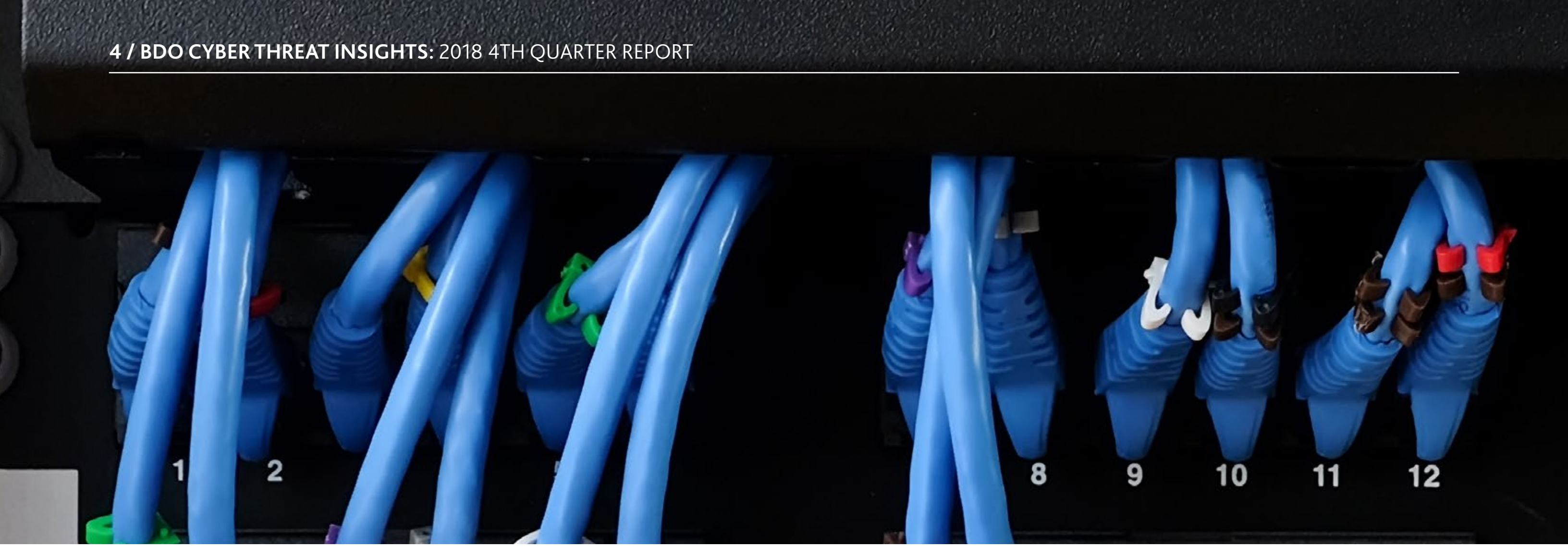
[9] https://www.whitehouse.gov/articles/american-technology-council-summit-modernize-government-services/

[10] https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf

[11] https://ifs.host.cs.st-andrews.ac.uk/Books/SE9/Web/LegacySys/Risks.html

[12] https://www.computerweekly.com/news/252445701/IT-meltdown-pushes-TSB-into-loss

Read more ▶



The new system was introduced by TSB's owner to give the bank the infrastructure required to harness the latest IT and become a challenger to the big high-street banks; however, the bank lost more than £100 million due to the meltdown. So, although upgrading or replacing legacy systems is seen as a risky and costly gamble, not doing so is seen as the safer option. For many public sector organizations, it is more compelling to passively incur ongoing rigid costs in the long term, rather than actively choosing to incur massive, yet short-term costs that may improve efficiency.[13] This creates an environment in which governmental organizations only change or update their systems when there is no other choice.

Earlier this year, for example, it was revealed that nearly half of councils in the UK are running outdated server software. After submitting Freedom of Information (FOI) requests[14], IT service provider Comparex UK[15] found that 46 percent of British local authorities' systems are still running outdated software such as Windows Server 2000, Windows Server 2003 and Microsoft SQL Server 2005.

But the opportunity cost of choosing to sustain the status quo is immense. According to a White House report[16] in the fiscal year (FY) of 2018, U.S. government-wide cost on operations and maintenance services for legacy systems accounted for 70 percent of the total IT budget[17] of $85.2 billion[18], compared to 68 percent in FY 2015. Even if the cost can be currently justified, that may soon change. Moreover, operational knowledge of legacy systems can be lost as employees who have historically maintained them retire and cannot be replaced.

Maintaining legacy systems can also mean maintaining outdated technology that is more vulnerable to attacks. The British government understood this when it signed a multi-million-dollar deal with Microsoft to upgrade all software in the National Health Service (NHS). This was part of a series of measures taken following the 2017 WannaCry attack. [19]

[13] A joint research by McKinsey and Oxford University, showed that large IT projects run 45% over budget, while delivering 56% less value than predicted - https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/delivering-large-scale-it-projects-on-time-on-budget-and-on-value

[14] https://www.infosecurity-magazine.com/news/half-of-english-councils-running/

[15] https://www.comparex-group.com/web/uk/en/comparex.htm

[16] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/budget/fy2018/ap_16_it.pdf

[17] https://itdashboard.gov/

[18] According to the official US budget website (see footnote 21) the IT budget is defined as "Government-wide IT Spending - the total budgetary resources based on development, modernization, and enhancement (DME) and operations and maintenance (O&M) services for the current fiscal year." Note that the budget does not include classified IT spending or the IT Modernization Fund (www.tmf.cio.gov).

[19] https://digital.nhs.uk/services/data-security-centre/data-security-centre-latest-news/boost-to-nhs-cybersecurity-as-new-security-measures-announced

Read more ▶

Cybersecurity - Under-Staffed, Under-Skilled and Under-Informed

Another problem is the sector's difficulty in recruiting and retaining quality IT and cybersecurity personnel, especially compared to the private sector.[20] This has greater impact on small agencies, which often then lack staff resources and technical expertise to securely operate existing systems, implement new platforms and adequately acquire security solutions.[21]

In July, the UK's Joint Committee on the National Security Strategy published an initial report regarding cybersecurity skills in critical infrastructure (CNI).[22] It found that the government does not have the ability to understand, and therefore address, the acute cybersecurity skill gap.

Exacerbating this is the discontinuity caused by the absence or change of expert leadership roles in government and the consequent effect on policy, recently illustrated by the changes in two key U.S. cybersecurity policy and management leadership roles: national security advisor[23] and cybersecurity coordinator. The latter specifically oversaw federal government cybersecurity and was critical in developing cross-agency policies.[24]

Furthermore, in some countries, policymakers generally lack the basic fundamentals of technology. For example, Japan's newly appointed cybersecurity minister admitted he never used a computer. Furthermore, he was unable to answer a question by the press regarding the use of USB drives with the country's nuclear power stations.[25]

While this example may be the exception rather than the rule, it is indicative of the advanced technological illiteracy in some aspects of public sector.[26]

This is less of a problem if there is a mechanism to provide public officials with in-depth, nonpartisan and objective analyses on technological matters. Unfortunately, many countries do not have such a body. In 1995, due to budget cuts, the U.S government did away with the agency whose job was exactly that: The Office of Technology Assessment (OTA). Unlike other congressional information agencies such as the GAO[27], which primarily evaluates ongoing programs, and the Congressional Research Service (CRS) that provides policy and legal analysis[28], OTA provided more comprehensive and technical analyses. In its lifetime, it proved a crucial resource for congressional members and staff on technological issues with regards to creating public policy.

However, awareness of the problem is beginning to shift. Recently, on Nov. 16, 2018, President Trump signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018. This legislation elevates the mission of the former National Protection and Programs Directorate (NPPD) and establishes the Cybersecurity and Infrastructure Security Agency (CISA) at a time when many nations have or are expected to formally do the same.

[20] https://www.forbes.com/sites/forbestechcouncil/2018/08/29/what-government-organizations-can-learn-from-the-private-sector-about-cybersecurity/#3ab02a282d9d

[21] https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf

[22] https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/706/706.pdf

[23] https://www.nbcnews.com/politics/politics-news/tom-bossert-trump-s-homeland-security-adviser-resign-n864321

[24] https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html

[25] https://www.independent.co.uk/life-style/gadgets-and-tech/news/yoshitaka-sakurada-japan-cybersecurity-minister-computer-not-used-a8635226.html

[26] https://www.wired.com/2016/04/office-technology-assessment-congress-clueless-tech-killed-tutor/

[27] https://www.gao.gov/

[28] http://www.loc.gov/crsinfo/

Read more ▶

Facing Evolving Cyber Threats in the U.S. and Canada

Organizational issues in conjunction with infrastructural failings create an operational reality that systematically constrains governments' ability to respond effectively to cyber threats, both on federal and local levels. For instance, throughout 2017 and 2018, numerous cities globally fell victim to various types of cyberattacks[29] such as ransomware and denial of service (DoS). Two notable incidents are the attacks on Atlanta and Baltimore in March that disrupted vital services. In the case of Atlanta, recovery efforts have been estimated at $17 million.[30]

This is becoming a growing cause for concern in the development and adoption of "smart" infrastructure that can monitor and gather an unprecedented amount and quality of data. For instance, in March, Toronto and Alphabet (Google's parent company) received backlash[31] after they didn't provide answers regarding the security framework for their joint smart city project "Sidewalk Labs".[32] In October, two key members of the program, including Ontario's privacy commissioner, resigned over surveillance and data privacy concerns blatantly disregarded by the company and the city.[33]

These concerns are well-justified, especially where smart infrastructure is or will be connected to critical systems. Despite constant reassurances, regular incidents demonstrate how the public sector struggles with current threats and new attack vectors.

ONWASA Hit by Polymorphic Trojan

On Oct. 4, Onslow Water and Sewer Authority (ONWASA)[34] was hit with a variant of a polymorphic trojan known as EMOTET.[35] Polymorphic malware is an advanced and modular malware that obfuscates its activity by constantly changing its identifiable features. The initial attack was believed to have been resolved; however, due to ongoing and persistent problems, ONWASA's IT staff contacted external security experts to assist them.[36] Nevertheless, despite the added security measures and personnel, ONWASA was hit again on Oct. 13 by a sophisticated ransomware dubbed RYUK.[37] The IT and security team promptly took the systems offline, but by that point, the malware already infected and encrypted databases and files.

ONWASA decided not to pay the ransom, and as a result, had to rebuild several of its databases. To prevent significant disruption, it was forced to continue its operation manually. Regarding the identity of the attacker, RYUK ransomware, which shares code with the Hermes malware, was previously linked to the North Korean APT Lazarus. Although this attack did not result in significant damages, it is just one of the latest attacks targeting critical systems.

[29] https://community.spiceworks.com/topic/2124589-not-just-atlanta-ransomware-strikes-dozens-of-u-s-cities-in-2017-and-2018

[30] https://www.beckershospitalreview.com/cybersecurity/atlanta-s-ransomware-attack-may-cost-the-city-17m.html

[31] https://www.cbc.ca/news/technology/sidewalk-labs-toronto-neighbourhood-alphabet-google-privacy-1.4585534

[32] https://www.sidewalklabs.com/

[33] https://www.ctvnews.ca/sci-tech/sidewalk-labs-consultant-resigns-over-data-protection-concerns-1.4143342

[34] https://www.onwasa.com/

[35] https://www.us-cert.gov/ncas/alerts/TA18-201A

[36] https://www.onwasa.com/DocumentCenter/View/3701/Scan-from-2018-10-15-08_08_13-A

[37] https://threatpost.com/ryuk-ransomware-emerges-in-highly-targeted-highly-lucrative-campaign/136755

Read more ▶

Large-Scale Attack on Ukraine's Power Grid

Perhaps the most noteworthy event of this sort is the large-scale attack on Ukraine's power grid in late 2015.[38] This was one of the most sophisticated and significant cyberattacks in recent years, with ramifications still being felt today. As the attackers did not destroy the power grid, despite having the capabilities to do so, researchers believe the attack was executed as a Proof of Concept (PoC). Notably, it was used as a testbed to better develop the attacker's skills, tools and knowledge for future attacks against other countries.[39] Nonetheless, it also illustrated the threat on critical infrastructures and brought attention to the required measures the public sector must undertake to prevent reoccurrences of such attacks.

Lessons Not Learned by Government Agencies

Regretfully, however, we often also see that even after critical attacks, many governmental bodies still fail to take the necessary measures needed to protect sensitive assets going forward. The 2015 U.S. Office of Personnel Management (OPM) breach that compromised sensitive records of more than 21 million people[40] is estimated to cost the government more than $1 billion over the next decade.[41] Despite the cost and threat to national security, though, it's three years later, and OPM has not yet implemented the necessary changes to protect itself. Of the 80 recommendations made by GAO, more than one-third remain open as of late November 2018.[42]

While this is perhaps an egregious case, it is emblematic of the global public sector's difficulty in making the necessary changes. It should be emphasized that more than a matter of resources, it is the public sector's systematic and pervasive hardship in adopting fundamental cybersecurity frameworks.

Supply Chain Attacks on the Public Sector

Although many attacks are executed for monetary gain, they could also be used to disguise other malicious activities, as is often the case to the supply chain, which is considered the weakest link (e.g., third-party providers or contract workers). This can be achieved via any number of vectors, including spear phishing and waterhole attacks, to obtain an entry point into even a highly secure government organization.

This was the case in the 2017 NotPetya attack on Ukraine, which was executed via an accounting software provider MeDoc, widely used both by the private and public sector in Ukraine.[43] Similar to WannaCry, the propagation vector was not email. Instead, NotPetya was disseminated via a weaponized software patch issued by its official updater.

Further, the attack hid its true intention. While the malware did encrypt systems and demanded ransom, the attackers did not seek financial gain. Instead, the intent was sabotage aimed at wiping/corrupting infected computers' hard drives by erasing the Master Boot Record. As a result, even if the hard drive is restored, the files cannot be recovered. In total, about 2,000 companies and organizations were affected, and amongst them, governmental offices around the world.

CONCLUSIONS

Malicious actors are becoming increasingly proficient in executing attacks on a wide gamut of industries, including critical infrastructure. As technology evolves, it is creating bridges between industries, geographical locations and, therefore, potential victims of cyberattacks. In its current state, the public sector is largely unable to efficiently coordinate operations in real or near-real time across multiple platforms and channels[44] to adequately protect itself against evolving threats.

[38] https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

[39] https://www.wired.com/story/russian-hackers-attack-ukraine/

[40] https://www.opm.gov/cybersecurity/

[41] https://www.symantec.com/connect/blogs/opm-breach-costs-could-exceed-1-billion

[42] https://www.gao.gov/assets/700/695368.pdf

[43] https://blog.talosintelligence.com/2017/07/the-medoc-connection.html

[44] https://www.nap.edu/read/18749/chapter/7

Read more ▶

Public Sector - Notable Attacks and Events in 2018

CHINESE HACKERS TARGET NATIONAL DATACENTER IN A SOPHISTICATED ESPIONAGE CAMPAIGN

On June 13, Kaspersky Lab reported[45] an ongoing country-level waterholing campaign against an unnamed country in Central Asia. The campaign, executed by APT27 (aka LuckyMouse and EmissaryPanda), compromised a key national datacenter, providing the attackers with "access to a wide range of government resources at one fell swoop." The campaign is believed to be active since at least autumn of 2017. According to the report, the attackers leveraged this access to execute waterhole attacks via an unspecified number of the country's official websites, which were injected with malicious scripts. The weaponized sites would then direct and redirect visitors to instances of both ScanBox and BeEF (The Browser Exploitation Framework). ScanBox is a reconnaissance framework that gathers data regarding the victim's machine, while the latter, BeEF, is a "penetration & testing tool that focuses on the web browser."[46] It should be noted that the initial infection vector is still unclear. However, one of the tools found in this campaign is a variant of the HyperBro Trojan, which is regularly used by various Chinese-speaking actors.

NATION-STATE APT ATTACKS TARGET DEFENSE CONTRACTORS

APT15 Steals Military Documents from UK Government Contractor

A Chinese-affiliated threat agent APT15 has reportedly penetrated the systems of a UK government contractor, effectively gaining access to highly sensitive military technology information, according to a report by NCC Group published on March 10, 2018.[47] The incident in question was discovered in May 2017, when a contractor providing a range of services to the British government suffered a network breach. NCC Group's analysis of the incident yielded that two new backdoors, dubbed RoyalCli and RoyalDNS, were used by the actor, as well as BS2005, a tool previously affiliated with APT15. APT15 operated on the compromised network from May 2016 until late 2017 and affected more than 30 hosts during that time. The initial point of entry into the network remains unclear; however, the attackers gained domain administrator credentials by using the open-source tool Mimikatz, which later facilitated the seizure of a VPN certificate which was then used to access the victim's network remotely.

[45] https://securelist.com/luckymouse-hits-national-data-center/86083/

[46] http://beefproject.com/

[47] https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

Read more ▶

Chinese Hackers Stole 614GB of Data from a U.S. Navy Contractor

In early June, it was reported that between January and February, hackers linked to the Chinese government stole 614GB of highly sensitive data from an unnamed contractor that possibly included plans for a supersonic anti-ship missile intended to be operational by 2020. According to The Washington Post, the hackers also stole material related to a "project known as Sea Dragon, as well as signals and sensor data, submarine radio room information relating to cryptographic systems, and the Navy submarine development unit's electronic warfare library."[48]

The Post claims that further data was compromised; however, at the request of the Navy, it is withholding reporting any details about it to avoid harming national security. It should be noted that the data was hosted on an unclassified network. Furthermore, while the compromised data is described as "highly sensitive," official sources have stated that when aggregated, it could be considered classified. The breach is being investigated jointly by the Navy and the FBI. As of writing this report, no technical information regarding the attack vector or tools has been revealed.

Chinese APT Targets U.S. Satellite and Defense Companies

A Chinese group has been targeting satellite, communications, geospatial imaging and defense organizations in the United States and Southeast Asia, for espionage and/or sabotage purposes, according to a Symantec report from June 19, 2018.[49] In the latest wave of attacks beginning in 2017, the group named Thrip by Symantec, targeted a satellite communications operator and an organization involved in geospatial imaging and mapping. Notably, the group seemed to focus on the operational side of these companies, and deliberately sought to infect systems running software that monitor and control satellites and geospatial imaging applications. This focus suggests the threat actor likely had a destructive motive. In addition to these targets, this threat actor also targeted three different telecom operators based in Southeast Asia and a defense contractor.

Thrip uses a wide range of tools and custom-made malware on its targets. However, the group is increasingly relying on living off the land tactics and open-source tools. This renders the malicious activity more difficult to detect and attribute, as it blends in within a large number of legitimate processes. In this campaign, the actor employed a previously unknown custom Trojan called Catchamas, an information stealer that contains additional features designed to avoid detection.[50]

Catchamas is built to obtain various types of information from infected computers, including keystrokes, clipboard data and screenshots based on specified keywords in the window title and network adapter information. Moreover, Thrip used an updated variant of Rikamanu, an attributed Trojan that logs on to a compromised computer.[51] It also leveraged PsExec, a legitimate Microsoft Sysinternals tool for executing processes on other systems, to install the malware and move laterally on the compromised networks. Additionally, it used the following legitimate/open-source tools:

- **PowerShell:** A Microsoft scripting tool used to run commands to download payloads, traverse compromised networks and carry out reconnaissance.
- **Mimikatz:** A freely available tool capable of changing privileges, exporting security certificates and recovering Windows passwords in plaintext.
- **WinSCP:** An open source FTP client used to exfiltrate data from targeted organizations.
- **LogMeIn:** A cloud-based remote access software.

[48] https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?noredirect=on&utm_term=.a64f5945b9d9

[49] https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets

[50] https://www.symantec.com/security-center/writeup/2018-040209-1742-99

[51] https://www.symantec.com/en/sg/security-center/writeup/2015-072710-4212-99

Read more ▶

Third-Party Service Provider Data Breach Compromises Sensitive Pentagon Staff Records

On Oct. 12, the Pentagon issued a statement in which it revealed that it fell victim to a cyberattack compromising sensitive U.S. military and civilian personnel.[52] According to the statement, an unnamed contractor providing travel management services to the Department of Defense was hacked. The breach potentially compromised personal information and credit card data of up to 30,000 individuals. The breach was discovered on Oct. 4. According to the Pentagon, the breach affected a single vendor that provided services to a small portion of the total population.

As of late November, no additional information was revealed regarding the attack. While this incident appears to have been quickly contained, it does highlight the potential risk from supply chain attacks. Chiefly, that compromised data could be leveraged in a number of vectors, including spear phishing attacks, to obtain an entry point and foothold for an otherwise highly secure organization.

Northern Irish Parliament Assembly Mailboxes Targeted by Hackers

The Northern Irish Parliament Stormont fell victim to a partially successful penetration of its assembly mailboxes by unknown attackers.[53] Stormont's IT department instructed staff to promptly change their mail passwords and report any further suspicious activity. The accounts that were successfully hacked by the attackers have been disabled. The Parliament informed its staff of the attack in an email that was viewed by reporters. The notification apparently stated that Stormont's IT teams were collaborating with Microsoft and the National Cybersecurity Center to address the cyber event.

Cyberattacks Hit Public Transport in Denmark

In early May, two nationally owned public transport operators in Denmark were hit by cyberattacks affecting thousands of commuters in the country. In the first incident, an overnight attack on Copenhagen's electric city bike system shut down thousands of electric bikes in the capital city, forcing residents reliant on the service to turn elsewhere.[54] Several days later, on May 13, the largest Danish train operator was hit by a Distributed Denial of Service (DDoS) attack that prevented customers from making purchases on the company's various ticket sales platforms.[55] The DDoS attack on Danske Statsbaner (DSB) prevented customers from buying tickets on the operator's app, ticket machine, website and stores. Moreover, the company's internal email and telephone systems were also affected in this attack, rendering staff unable to communicate with other staff or customers. DSB estimated that the attack affected about 15,000 customers, though passengers were still able to buy tickets from staff on board the trains. The company resolved the issue one day later and notified law enforcement about the incident.

An internal investigation of the attack revealed it was carried out by an external actor who attempted to bring the company's system down. The company did not disclose further information about the attacker's identity or the motive behind the attack.

[52] https://www.washingtonpost.com/politics/federal_government/pentagon-reveals-cyber-breach-of-travel-records/2018/10/12/fed2ced2-ce60-11e8-ad0a-0e01efba3cc1_story.html?noredirect=on&utm_term=.b83ca5b004a9

[53] http://www.bbc.com/news/uk-northern-ireland-43558156

[54] https://www.hackread.com/copenhagen-citys-bicycle-sharing-system-hacked

[55] http://www.transportsecurityworld.com/ddos-attack-cripples-danish-rails-ability-to-sell-tickets

Read more ▶

Ransomware Infects the Hong Kong Department of Health

Hong Kong's Department of Health (DOH) was hit in late July by ransomware that encrypted three of its computers. The unidentified attacker left behind an email address to contact for a decryption key, but interestingly, no ransom was demanded.[56] Despite this fact, investigators believe that profit was the motive behind this incident.

In a statement on August 3, 2018, a spokesperson for the DOH announced that three of the department's computers were infected with ransomware that rendered data inaccessible. The infection occurred sometime in the two weeks since July 15, 2018. The impacted computers belonged to the DOH's Infection Control Branch, Clinical Genetic Service and Drug Office, and investigators believe the initial infection vector was a malicious attachment to an email sent to an employee.

According to the DOH's statement, the computers did not contain any confidential personal information and no data had been leaked. Moreover, the department had an offline backup of all the data stored on the infected computers. The DOH reported the incident to the relevant local authorities and is currently investigating the circumstances that led to it.

Ransomware Attacks on U.S. Municipalities

Notable ransomware attacks were launched in March 2018 on Atlanta and Baltimore, along with an attack on the port of San Diego in late September 2018, that disrupted vital services. The city of Atlanta was hit by SamSam ransomware which exploits a deserialization vulnerability in Java-based servers.[57] The attackers compromised a vulnerable server first, and ransomware spread to desktop computers throughout Atlanta's entire network. Many of the city's online services were crippled for six days, with some workers resorting to using pen and paper. Three months after the attack, a third of the city's 424 software programs were still offline or partially inoperable.[58]

The attacker demanded a ransom of $55,000 in bitcoin but was never paid. Recovery efforts have since been estimated at $17 million. In contrast, prior to the attack, the Atlanta government was criticized for its lack of spending on IT infrastructure upgrades.

SamSam differs from other ransomware in that it does not rely on phishing, but instead uses a brute-force attack to guess weak passwords until one breaks open. It is known to target weaker IT infrastructures and servers.[59] This ransomware has prominently been behind attacks on medical and government organizations since its discovery in 2016, with previous attacks on targets ranging from small towns such as Farmington, New Mexico, to the Colorado Department of Transportation and the Erie County Medical Center in Buffalo, New York. To date, the identity of the SamSam hackers remains unknown.[60]

The attack elevates the question of whether paying a ransom is the right choice. The official government guidelines are against paying ransoms, as to not encourage attackers to execute them. Hackers often demand relatively small amounts of money to make the option of paying the ransom more favorable. This makes the choice of whether to pay ransom or not even more difficult, as the cost in paying the ransom is much lower than combating it.

[56] https://latesthackingnews.com/2018/08/05/hong-kong-health-department-computers-hit-by-cyber-attack/

[57] https://www.zdnet.com/article/atlanta-spent-at-least-two-million-on-ransomware-attack-recovery/

[58] https://www.infosecurity-magazine.com/news-features/top-ten-atlantas-ransomware/

[59] https://statescoop.com/atlanta-was-not-prepared-to-respond-to-a-ransomware-attack/

[60] https://www.csoonline.com/article/3263693/security/samsam-ransomware-attacks-have-earned-nearly-850-000.html

Read more ▶

CASE SPOTLIGHT

Malware Attack on German Foreign Ministry

In early September, Antivirus and Internet Security Solutions (ESET) published a follow-up investigation report about the attack on the German Foreign Ministry[61] attributed to Russian nation-state actors. The attack was notable for the unique backdoor that was used, which does not require a direct Internet connection to operate. Instead, the backdoor can leverage the ability to send emails from workstations and compromise controlled environments that maintain a highly filtered Internet connection. The backdoor mainly targets users of Microsoft Outlook, a widely used mail client, but also targets The Bat!, an email client used across Eastern Europe.

OVERVIEW OF THE EVENT

The attack, which began in 2016 and was identified by the German authorities only in late 2017, resulted in the exfiltration of sensitive data for more than a year and is attributed to Turla (sometimes referred to as Snake), a Russian cyberespionage threat group. The actor obtained access to the German Foreign Ministry's computer infrastructure via malware that communicates with its command-and-control server through specially crafted PDF documents attached to emails. It's worth noting that the backdoor operates on common protocols; however, it does not exploit any actual vulnerabilities in PDF Reader or Outlook. Rather, the malware is able to decode data from the PDF documents and interpret it as commands for the backdoor.

PENETRATION VECTOR

Initially, the attackers infected the network of the Federal Academy of Public Administration (Hochschule des Bundes), a federal administrative university. The attackers then laterally moved across the network until they successfully achieved persistency in March 2017. The most notable tool in the attack is the aforementioned Turla backdoor, which appears to have been used since 2013 and was created as early as 2009. In addition to the attack on the German Foreign Ministry, this backdoor was involved in attacks on two additional European governmental institutions and a major defense contractor. We assess with moderate certainty that one of the targets was the French government. This is based on a string found within the malware that contained the official French government top-level domain (TLD), *gouv.fr*.

[61] https://www.welivesecurity.com/wp-content/uploads/2018/08/Eset-Turla-Outlook-Backdoor.pdf

Read more ▶

MALWARE ANALYSIS

The backdoor has a number of variants, several of which target Outlook's email client, while others target The Bat!. The command-and-control protocol is based on sending and receiving emails from the attackers' email addresses. These emails are attached with PDF files containing commands for the malware or data taken from the compromised systems and siphoned off to the attackers. The commands are compressed with bzip2 and encrypted with a modified MISTY1 algorithm. The communication with the malware is fully transparent to the user, and the emails are timed and sent to the attackers at the same time the user sends a legitimate email—reducing the chances of detection.

In 2018, the backdoor gained the ability to run PowerShell commands via a tool named Empire PSInject,[62] which injects PowerShell commands into the process. Due to the design of the command and protocol, the backdoor does not require direct access to the Internet—only a workstation capable of sending emails. Accordingly, this malware poses a risk to controlled environments with highly filtered Internet connections. Moreover, shutting down the attacker's email address does not hinder the malware's command-and-control capabilities as it does not verify the identity of the sender. Accordingly, it can be controlled from any email address. This does mean, though, that more than one group may be using it.

Moreover, Turla created a different email address for the command-and-control function of each target. This was done via the free email service GMX by using real employees' names based on the following format: *firstname.lastname@gmx[.]com*

The use of GMX and employees' names presents several mitigation issues. Firstly, most organizations would prefer not to block the domain gmx.com. Secondly, it can be difficult to tell the difference between the malicous emails and legitimate private email accounts of the emplolyees. Thirdly, the backdoor does not exploit a vulnerability in Outlook, but rather uses the software in a legitimate way via Microsoft's API – MAPI.[63] It manages to avoid authenticating the user's email account by exploiting his or her previous open session.

PERSISTENCY

In the case of the Outlook variants, the malware hijacks the COM[64] to obtain persistency, while modifying certain CLSID[65] values in the Windows Registry. This results in the execution of the DLL during each reboot of the client's software. It should be noted that in Windows OS, there is a security mechanism designed to prevent the redirection of COM objects to malicious DLL files based on the integrity level of the process. Namely, if the integrity level of a process is higher than medium, the COM runtime ignores per-user COM configuration and accesses only per-machine COM configuration. Nevertheless, in this scenario, this feature fails, as Outlook's process runs at medium-integrity level. Moreover, COM referrals do not require Admin authorization.

In the case of The Bat!, the threat actors registered a plugin to the client's software that executed the malicious DLL file each time it was opened. The registration of a plugin for The Bat! consists of modifying the following configuration file: %appdata%\The Bat!\Mail\ TBPlugin.INI. There is no preset path for the Turla Backdoor's DLL file. As such, it can be located anywhere on the hard drive.

RECOMMENDATIONS

Create alerts for anomalies by:

- Blocking emails with PDF attachments sent from the domain gmx.com
- Monitoring and flagging emails with certain subjects sent simultaneously from the same user
- Statistically examining abnormal email sending patterns from the organization's email address, attached with PDF files
- Disabling the option of sending encrypted emails (creating an alert for emails containing bzip2 compressed data, or data encrypted by modified algorithms associated with Turla – MISTY1, CAST-128, RSA and ThreeFish)
- Creating a rule in the email filter system that blocks and alerts of any email that does not contain a pre-defined character or feature (e.g., a specific file attachment or special notes/characters)

[62] https://github.com/EmpireProject/PSInject

[63] Messaging Application Programming Interface.

[64] Microsoft Component Object Model - a platform-independent, distributed, object-oriented system for creating binary software components.

[65] Class Identifier – a unique global identifier of COM objects, which is comprised on a 128-bit long number and coded in Hexadecimal and recorded on Windows Registry.

Read more ▶

City of Tyler, Texas Hit by Data Breach Linked to Click2Gov Utility Payment Platform

The city of Tyler, Texas notified customers who used the one-time utility payment option through Click2Gov from June 18 to August 21 about yet another data breach linked to the online payment system. The city announced the breach on September 10, 2018, and clarified it is in the process of identifying and contacting all potentially affected individuals.[66]

According to the city's statement, personal information affected by the incident includes payment card information (card number, security code and expiration date), full names, address, city, state and zip code. This event is just the latest in a series of security breaches across dozens of U.S. cities that have been linked to the Click2Gov platform by the Florida-based company Superion.[67]

These include the following cases:

- On February 28, 2018, the city of Thousand Oaks, California learned of unauthorized access to its online payment system Click2Gov, exposing payment card details for transactions between November 21, 2017 and February 26, 2018.
- On May 25, 2018, Oxnard, California was notified by a bank that its online utility bill payment service was breached, and transactions taking place between March 26 and May 29, 2018 were exposed. Click2Gov was the payment processing application involved.
- On June 6, 2018, Wellington, Florida, was notified by Superion that certain vulnerabilities in Click2Gov may have led to a breach of its online utility payment installation. While a breach was not confirmed, Village announced that payment card data used for online bill payments between July 2017 and February 2018 is considered to be at risk.
- On October 11, 2017, Ormond, Florida was alerted to a problem by a credit card issuer after customers detected fraudulent activity while using their credit cards to pay utility bills online. In fact, customers had been reporting fraudulent charges they believed to be linked to the city since September 22 that year.

In a statement earlier in 2018, Superion reported that after its clients started noticing suspicious activity, it "took proactive steps" to notify customers and hired a forensic investigator to determine the source of the data breaches. According to the company, the source of the data breaches traces back to vulnerabilities in a third-party vendor, Oracle's WebLogic application server.[68]

[66] https://www.databreaches.net/click2gov-payment-system-security-breach/

[67] https://www.riskbasedsecurity.com/2018/06/click2gov-or-click2breach/

[68] https://www.axios.com/newsletters/axios-codebook-cc279715-4e41-43a7-99f3-c6f5d1a0237f.html

Read more ▶

National Cybersecurity Strategic Plans: Country-Specific Spotlights

Australia

In April 2016, Australia launched its national cybersecurity strategy. The strategy built upon the country's 2009 Cybersecurity Strategy and broke a seven-year government silence on cybersecurity strategy matters. In April 2017, the strategy saw its first annual update.

The overall goal of Australia's Cybersecurity Strategy is to enable innovation, growth and prosperity for all Australians through strong cybersecurity practices. To do this, the strategy establishes five interdependent but structured themes:

1. Strong cyber defenses, which include:

- Promoting the adoption of the Australian Signal Directorate (ASD) / Department of Defense's "Essential 8" cybersecurity controls and offensive cyber capabilities
- Provision of $300 to $400 million in funding for cybersecurity initiatives over 10 years
- Increased capacity development for Australia's Computer Emergency Response Team (CERT)
- The establishment of Joint Cybersecurity Centers (JCSCs) in capital cities to facilitate industry collaboration on cyber threats and incidents

2. Global responsibility and influence, which includes:

- Appointing the Australian Ambassador for Cyber Affairs and developing The Cyber Cooperation Program and International Cyber Engagement Strategy to support Australia's cyber capacity-building efforts in the Indo-Pacific
- Appointing a Minister and Special Adviser for Cybersecurity to the Prime Minister of Australia
- Appointing an Ambassador for Cyber Affairs to lead Australia's international engagement on cybersecurity

3. Growth and innovation, which includes:

- Establishing the Australian Cybersecurity Growth Network (ACSGN) to provide a foundation for the development of next-generation cyber products and services.

4. A cyber-smart nation, which includes:

- Public awareness campaigns
- Academic centers of cyber excellence
- An annual Australian Cybersecurity Challenge initiative

5. A national cyber partnership, which includes:

- Senior engagement and leadership on cybersecurity issues
- Cyber threat intelligence sharing across private and public sectors

CONTACT:

LEON FOUCHE
National Lead, Cybersecurity - Australia
+61 7 3237 5688 / leon.fouche@bdo.com.au

Read more ▶

Germany

In February 2011, Germany's Federal Ministry of the Interior issued the Cybersecurity Strategy for Germany paper. The document describes cyberspace as "all information infrastructures that can be accessed via the Internet." The strategy connects the economic and social prosperity in Germany directly to an Internet that offers reliable and available information and communications technology, as well as the integrity, authenticity and confidentiality of data in cyberspace.

By creating the Cybersecurity Strategy, the federal government aims to make a substantial contribution toward securing cyberspace through a comprehensive approach mainly based on civilian services and supplemented by measures taken by the German Bundeswehr. The Cybersecurity Strategy takes into account the global nature of cyberspace and requires an internationally coordinated network in terms of security policies, including cooperation between United Nations and European Union member states, as well as the Council of Europe, NATO, the G8, the Organization for Security and Co-operation in Europe (OSCE) and other multinational organizations.

The following 10 strategic objectives and measures have been explicitly defined in the paper:

1. Protection of critical information infrastructures
2. Secure IT systems in Germany
3. Strengthen IT security in the public administration
4. National Cyber Response Center
5. National Cybersecurity Council
6. Effective crime control also in cyberspace
7. Effective coordinated action to ensure cybersecurity in Europe and worldwide
8. Use of reliable and trustworthy information technology
9. Personnel development in federal authorities
10. Tools to respond to cyberattacks

Read more ▶

The strategy was refined and updated in 2016 by the “federal government’s strategic framework relating to increased security in cyberspace” that comes in four fields of actions:

1. Safe and self-determined action in a digitized environment

- Increase awareness and competency in the digital field
- Establish secured electronic identities
- Create conditions for a secure cyberspace
- Install an IT security label and strengthen certificates and approvals
- Ensure that digitization is built secure
- Promote IT security researching

2. Joint effort of government and industry

- Secure critical Infrastructures defined in the IT Security Law from 2015
- Protect business in Germany
- Strengthen German IT economy
- Collaborate with providers for detection of anomalies
- Get IT security providers involved to exchange cybersecurity information
- Establish a trusted platform for secure information exchange between public and private sectors

3. Powerful and sustainable cybersecurity architecture at a national level

- Refine national Cyber Defense Center (Cyber-AZ), founded in 2011
- Strengthen the on-site response capabilities by establishing the “Mobile Incident Response Teams” (MIRT), which are part of the Federal Office for Information Security (BSI)
- Improve cyber forensics for investigations
- Fight cyber espionage and cyber sabotage
- Establish an early warning system from signals intelligence support to cyber defense (SSCD)
- Foundation of the central office for IT (ZITiS)
- Integrate cyber defense in all planning, structures and processes for overall defense
- Strengthen CERT structures
- Establish protection measures for the Federal Administration (UP Bund)
- Increase cooperation between states and the federation
- Recruit specialists for the federation, states and communes

4. Active positioning of Germany in European and international cybersecurity policy discussions

- Design an effective European cybersecurity policy
- Refine the NATO Cyber Defense
- Take an active role in creating cybersecurity on an international level
- Strengthen international law enforcement

CONTACT:

STEPHAN HALDER
National Lead, Cybersecurity - Germany
+49 40 30293-169 / stephan.halder@bdo.de

Read more ▶

Israel

Israel's Cybersecurity Strategy aims to achieve two core goals that encompass both domestic and international activities. The first is to secure cyberspace by confronting cyber threats. The second is to drive the rapid evolution of relevant technology and maintain Israel's scientific and technological capability and its position within the international community as a leading innovator and contributor. This includes supporting research, promoting industrial innovation and working to enhance the pool of human capital.

Israel's Cybersecurity Strategy is based on the "Concept of Operations" (ConOps), which integrates state actions to confront cyber threats with private-sector efforts to support security activities to achieve three parallel objectives:

1. Aggregate Cyber Robustness

Take specific steps to raise the standards of cybersecurity in government through the introduction of more advanced technology, including targeted efforts to promote knowledge and awareness within the private sector, with special attention to critical national infrastructure and regulation of the cybersecurity market to maintain standards of security professionals, technological services, and security products and solutions.

2. Systematic Cyber Resilience

The ability to confront and contain cyberattacks has been reinforced around the benefits of greater information sharing through the national computer emergency response team (CERT), which has engaged on a broader, global, pan-national basis.

Enhanced efforts have been made to gather and process threat intelligence, provide early warning through close direct collaboration with the private sector, and support organizations through identification and investigation of attacks and sector-specific Security Operations Centers.

3. National Cyber Defense

National cyber defense is implemented through a multi-faceted, multi-agency and coordinated national campaign in three parts:

- **Active defense** based on intelligence operations and deterrence activities directed against the sources of cyber threat.
- **More conventional Defensive Operations** comprising situational monitoring and assessment, detection and response.
- **Joint investigations** and enforcement operations with law enforcement.

CONTACT:

OPHIR ZILBIGER
Head of Cybersecurity Center, Israel
+972 52 6755544 / ophirz@bdo.co.il

Read more ▶

United States

In September 2018, the White House released the new "National Cyber Strategy of the United States of America." This new U.S. strategic plan is the first real one of its kind in the past 15 years.

The National Cyber Strategy communicates the following strategic imperatives:

1. Defend the homeland by protecting networks, systems and data
2. Promote American prosperity by developing a secure and thriving digital economy
3. Preserve peace and security by strengthening the ability of the United States, in concert with allies and partners, to deter and, if necessary, punish those who use cyber tools for malicious purposes
4. Expand American influence abroad via an open, interoperable, reliable and secure Internet

Key aspects of the new National Cyber Strategy include the following actions:

1. Secure Federal Networks & Information

- Centralize management and oversight of federal civilian cybersecurity under the DHS
- Align risk management and IT modernization under DHS leadership
- Improve federal supply chain risk management
- Strengthen federal government contractor cybersecurity

2.Secure Critical Infrastructure

- Prioritize public- and- private-sector coordinated cybersecurity actions for the critical infrastructure-designated industries
- Motivate private-sector investment to enhance cybersecurity capabilities
- Increase national research and development (R&D) in cybersecurity
- Improve cybersecurity in maritime and space sectors

3. Combat Cybercrime & Improve Incident Reporting

- Modernize electronic surveillance and computer crime labs
- Strengthen partner-nation law enforcement
- Improve apprehension of cyber criminals abroad

4. Invest in Next-Generation IT & Mobile Communications Infrastructure

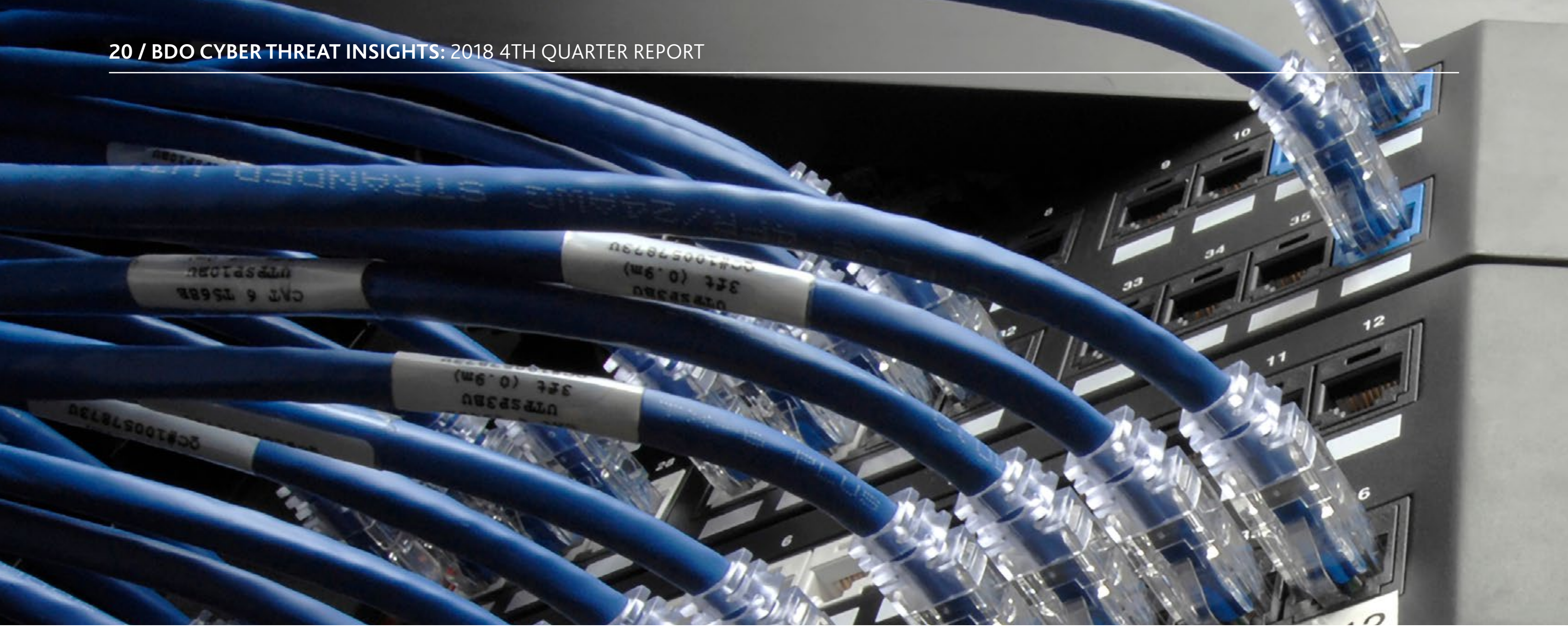
5. Maintain a Strong Intellectual Property (IP) Protection System

6. Enhance the Federal Cybersecurity Workforce

CONTACT:

GREGORY A. GARRETT, CISSP, CPCM, PMP
Head of U.S. and International Cybersecurity
703-893-0600 / ggarrett@bdo.com

Read more ▶



BDO Cybersecurity Services

Cybersecurity

PAYMENT CARD INDUSTRY (PCI)

- PCI assessment and remediation
- Third-party assessments

INFORMATION GOVERNANCE AND DATA PRIVACY

- Data mapping
- Data privacy assessments
- Data privacy strategy and implementation
- Privacy officer consulting
- Information governance assessments

CYBER INSURANCE

- Cyber insurance claim preparation
- Coverage adequacy evaluation

INCIDENT RESPONSE

- Data breach investigations
- Network/host active threat monitoring
- Threat hunting - exec, enterprise, nation state, insider
- Threat intelligence - deep/dark web, social media analysis
- Training & testing - 1st responder, table top, RED team, simulations
- IR data analytics

CYBER RISK ASSESSMENTS

- Level 1- 3 risk assessments against multiple frameworks
- Cyber risk remediation

CYBERSECURITY STRATEGY, POLICY AND PROGRAM DESIGN

- CIO & CISO advisory services
- Cyber strategy consulting
- Regulatory compliance
- Government relations consulting

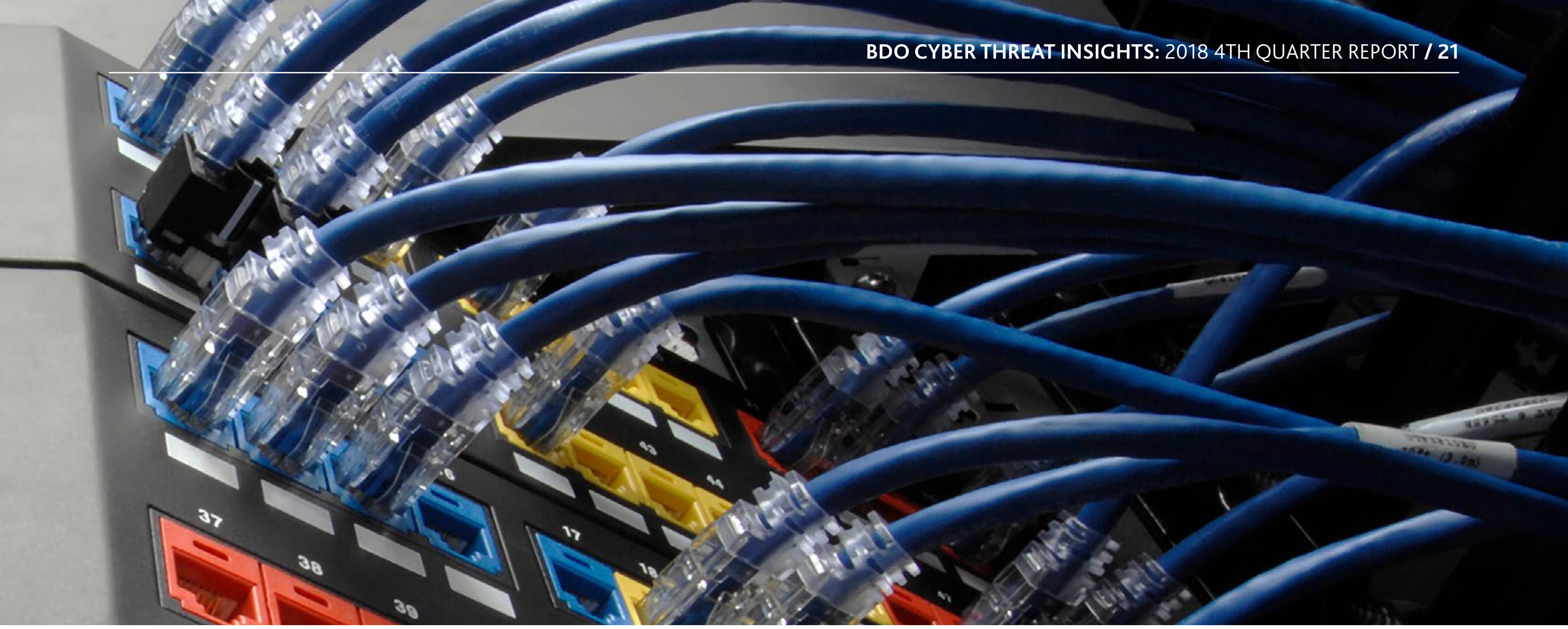
CYBER THREAT INTELLIGENCE

- Dark web recon
- Dark web analysis
- Social media

MANAGED SECURITY SERVICES

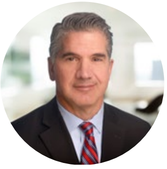
- Email and Network Attack Threat Assessments
- Security Operations Center (SOC)
- Penetration testing
- Vulnerability assessments
- Cloud migration & security
- Virtual desk-top services
- Cybersecurity education, training, & simulations
- Security Incident & Event Management (SIEM)

Read more ▶



U.S. Cybersecurity Leadership Team

GREGORY GARRETT
Head of U.S. & International Cybersecurity
703-770-1019
ggarrett@bdo.com



GREG SCHU
Partner
612-367-3045
gschu@bdo.com

MICHAEL STIGLIANESE
Managing Director
212-817-1782
mstiglianese@bdo.com

ANDREW SILBERSTEIN
Director
703-770-0537
asilberstein@bdo.com

LAURA HARS
Director
732 734-3059
lhars@bdo.com

MARK ELLENBOGEN
President/CEO of BDO Public Sector
703-336-1402
mellenbogen@bdo.com

JEFF WARD
National Managing Partner,
Third Party Attestation Services
314-889-1220
jward@bdo.com

ERIC CHUANG
Managing Director
202-644-5435
echuang@bdo.com

MICHAEL ADDO-YOBO
Managing Director
214-969-7007
maddo-yobo@bdo.com

FRED BRANTNER
Director
612-367-3129
fbrantner@bdo.com

Read more ▶

People who know Cybersecurity, know BDO.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.