Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **September 2021**
Sponsored by **Anomali**, **BIO-key International**, **KnowBe4**, **Mimecast**, **Progress MOVEit**, and **Virsec**

Cybersecurity in Government: Viewpoint 2021

Executive Summary

The term "government" covers a diverse collection of organizations in most countries—federal and central government agencies, state, local and tribal government organizations, municipalities, city councils, local law enforcement agencies, and more. With this variety comes a diversity of purpose, organizational size, attack attractiveness, and cybersecurity maturity across such organizations.

As an overall sector, government entities face a plethora of cybersecurity threats, including ransomware, business email compromise, phishing, and data breaches. Many are underprepared for the relentless onslaught of attacks. Currently, the single issue of highest concern across governments is susceptibility to ransomware attacks, both on systems like email and document sharing and critical infrastructure; the responsibility for the latter is often vested in private entities.

This white paper explores the current state of cybersecurity threats, preparedness, and response capability in the government sector. It offers direction to decision-makers and influencers working in the government sector on increasing the maturity and effectiveness of cybersecurity protections in government.

KEY TAKEAWAYS

The key takeaways from this research are:

- **Ransomware, ransomware, ransomware**
  The threat of highest concern across the government sector is ransomware, especially against critical infrastructure. Recent ransomware attacks against Colonial Pipeline and JBS have reverberated in governments around the world.
- **Susceptible to a diverse set of cyberattacks**
  Governments are under attack from a wide range of cyberattacks, including ransomware, phishing, business email compromise, data breaches, and misconfigured cloud storage accounts.
- **Governments represent an attractive target for cybercriminals**
  Cybercriminals go after the government sector to undermine citizen confidence, steal vital and classified data, and leverage systemic cybersecurity weaknesses against agencies.
- **Expect more ransomware and targeted attacks against symbolic agencies**
  Ransomware will continue to be a significant threat for government agencies. Cybercriminals will also continue to target agencies that carry symbolic meaning for the citizenry.
- **Solutions to consider for improving cybersecurity in government**
  Stronger identity protection with security controls such as multi-factor authentication, data encryption, data sharing methods, visibility into threats and incidents, threat intelligence services and sharing, and security awareness training (among others) are essential to improve cybersecurity readiness across government and shrink the likelihood of attacks being successful.

The threat of highest concern across the government sector is ransomware, especially against critical infrastructure.

ABOUT THIS WHITE PAPER

This white paper was sponsored by Anomali, BIO-key International, KnowBe4, Mimecast, Progress MOVEit, and Virsec. Information about each company is provided at the end of this paper.

Cybersecurity Threats in Government: Assessment

It is hard to secure an overall quantitative assessment on the scale of the cybersecurity problem in the government sector because many countries do not mandate notification of cybersecurity incidents and data breaches. Nevertheless, we can piece together an understanding of the types of attacks and threats in government by reference to published incidents and broader trends. In this section, we present a snapshot of what we know.

RANSOMWARE AGAINST INFRASTRUCTURE

Ransomware attacks have increased in frequency, consequential damage, and threat over the past several years,[1] and the volume of ransomware attack attempts in the first half of 2021 is 150% higher than the same time in 2020.[2] This year saw significant attacks on critical infrastructure (e.g., Colonial Pipeline, two wastewater systems in Maine[3]), food production (e.g., JBS[4]), and healthcare (e.g., multiple systems in the United States,[5] Ireland,[6] and New Zealand[7]), although government agencies have been hit as well (e.g., the city of Thessaloniki in Greece[8]). As we discuss later in this paper, these wider contextual attacks have garnered a response from federal and central government agencies around the world.

In the government sector itself, a recent survey found 40% of central government organizations had been hit with a ransomware attack during 2020, and for about half of these, their data was encrypted.[9] The same survey found that in local government, fewer organizations were hit with ransomware (34%), but a much higher proportion had their data encrypted (69%).

40% of central government organizations were hit with a ransomware attack in 2020.

RANSOMWARE WITH DATA EXFILTRATION

Over the past several years, ransomware gangs have added nefarious extras to their ransomware attack playbook to increase the likelihood of receiving a payment for their work. No longer assured of receiving a ransom payment if data is merely encrypted in place, gangs have added data exfiltration, threatened publication, auctioning sensitive data, and even engaging directly with victims discovered in breached data to demand ransom payment. In the government sector, ransomware attacks that also exfiltrated sensitive data occurred in:

- Mobile County, where systems were taken offline for three days to recover and over 90 GB of data was stolen, including personal data on all 1,600 county employees.[10]
- The Attorney General's office in Illinois. The incident occurred in April 2021 affecting personal data on Illinois citizens,[11] and the office was still largely offline at the end of July.[12]
- The city of Joplin in Missouri, which took more than a month to restore all affected systems and suppressed the publication of exfiltrated sensitive data by paying the ransomware demand via its cybersecurity insurance policy.[13]
- The Washington, D.C., Metropolitan Police Department. The ransomware gang published 250GB of stolen data when the department refused to pay the $4 million ransom demand.[14]

PHISHING

Few organizations in any industry sector do not receive phishing messages that attempt to steal credentials, exfiltrate data, plant malware, or redirect payments for payroll and outstanding invoices to a bank account controlled by the phisher as part of a scheme. Phishing attacks range from the broad-brushed to the highly targeted, and happen across email, social channels, messaging apps, and mobile devices. Phishing in the government sector currently has the following attributes:

- Heightened focus on stealing login credentials rather than planting malware. Stolen credentials can be used to provide ongoing access to a device, to enable data exfiltration, and to support lateral movement leading up to a ransomware detonation.[15]
- Phishing attacks against government targets is a global problem, with incidents reported against senior government officials in India,[16] federal government agencies in the United States,[17] and multiple state government agencies, for example in California.[18]

CONVERGENCE OF CYBER AND PHYSICAL THREATS

Cyberthreats and physical threats are increasing interacting, where one informs and shapes the other. For example, a potentially violent rally—a physical threat to a city or symbolic government building—is first organized using covert online discussions to attract participants, coordinate specific actions on the day of the rally, and ensure that everyone comes equipped with the right protest gear and weapons.[19] Actions in the physical world also result in cyberattacks, for example when hacktivists launch ransomware attacks against police departments in retaliation for police shootings and brutality.

Governments are heavily focused on this convergence and are tracking online threats to prepare for potential physical security events. At a state level, the purpose of a State Fusion Center—not to be confused with a commercial Cyber Fusion Center—is to collaborate with the numerous physical and cybersecurity agencies to identify, track, and mitigate threats across the cyber and physical domains.[20]

A business email compromise incident can cost a government agency $4 million.

MULTI-FACTOR AUTHENTICATION–RESISTANT PHISHING

Multi-factor authentication (MFA) has been found to decrease the likelihood of being subjected to a successful cybersecurity attack, particularly in the case of credential theft, account compromise, and remote access attacks. However, MFA is not immune to crafted attacks designed to bypass MFA protections,[21] with examples including SIM swapping, SMS hijacking, hijacked session cookies, and some phishing kits.[22]

BUSINESS EMAIL COMPROMISE

Business email compromise (BEC) attacks seek to divert payments for employee payroll and authorized invoices to a fraudulent bank account, or to fabricate payment demands for situations that are not real, e.g., a merger and acquisition in its early stages. BEC attacks result in the highest loss out of the 33 crime types tracked by the FBI, at 43% of overall crime losses during 2020.[23] In the government sector, the FBI has seen BEC incidents in recent years resulting in losses of up to $4 million per incident.[24] The FBI has not released incident details nor named specific government entities.

DATA BREACHES DUE TO PHISHING AND IT SYSTEM FAILURES

Most data breaches in the government sector are a consequence of email phishing attacks.[25] Compromised email account credentials provide access to items in the Sent folder, and anything else stored in the mailbox. Examples include the personal data of 58,000 unemployed persons in Florida,[26] and personal data of more than 9,000 people following a phishing attack at a state government agency in California.[27] Data breaches have also been tracked to IT system failures, such as what happened at the Oxford City Council in the United Kingdom where some quarterly rent statements were sent to the wrong address.[28]

WEAK ACCESS CONTROL PROTECTIONS

Weak access control mechanisms—such as easy-to-guess or shared passwords—were implicated in several attacks against water treatment plants during 2021, including Oldsmar in Florida[29] and a large water district in Southern California.[30]

MISCONFIGURED CLOUD STORAGE ACCOUNTS

Government agencies using cloud storage accounts run the risk of access control being misconfigured (or ignored entirely), enabling open access to data. Incidents in 2021 included the discovery of over 1,000 GB of sensitive and confidential data on citizens in Massachusetts, Connecticut, and New Hampshire due to misconfigured Amazon S3 buckets related to the use of mapsonline.net by cities across the three states,[31] 1.9 million records in a secret terrorist watchlist—including no-fly status—left accessible on a password-free and search engine–indexed ElasticSearch cluster,[32] and personal data on 750,000 Indiana residents who had taken an online contact tracing survey for the State Department of Health.[33]

RELIANCE ON EMAIL FOR TRANSFERRING AND SHARING FILES

The use of email as the primary means of transferring documents containing sensitive information raises several cybersecurity threats, including accidental misdirection of the original by sending it to the wrong person, unauthorized access to items in the Sent folder in an email account following credential theft, and unauthorized access to all messages and attachments stored in the email account—project documentation, sensitive data on people and citizens, organizational strategy thinking, and more. The move to the cloud for email services has seen people gain access to 50GB and 100GB mailboxes. Whether originating from a phishing attack, brute-forcing a password, or another type of compromise, several of the data breaches profiled in this section have been centered on compromised email accounts.

SUPPLY CHAIN COMPROMISE

Several supply chain attacks have impacted government agencies over the past year. Government agencies caught up in the SolarWinds attack included the United States Department of Justice,[34] United States Department of Homeland Security, the United States Federal Aviation Administration, and the United States Department of Energy, among many others.[35] The United States Agency for International Development was also affected, where a compromised email account was used almost six months after the initial attack at SolarWinds to launch a targeted phishing campaign against 3,000 email accounts at 150 government agencies, think tanks, consultants, and NGOs.[36] Downstream effects also cascaded from the compromise at the Department of Justice in the form of compromised email accounts at 27 United States attorneys' offices.[37] Another major supply chain

The supply chain attack at SolarWinds continues to have ramifications for U.S. federal government agencies.

attack—at Kaseya—infected between 800 and 1,500 businesses with ransomware. However, it remains unclear how many government agencies were compromised.[38]

UNPATCHED VULNERABILITIES IN APPLICATIONS

Cybercriminals seek ways of exploiting unpatched vulnerabilities in commonly used applications, particularly when it enables them to gain a foothold in the network, steal credentials, or breach data. For example, four vulnerabilities in Microsoft Exchange Server were exploited at the start of 2021 to compromise hundreds of thousands of organizations around the world, including thousands of government entities.[39] Government agencies that acknowledged being compromised were the Norwegian Parliament[40] and the European Banking Authority.[41] The U.S. Cybersecurity Infrastructure and Security Agency (CISA) issued an emergency directive with mitigation instructions for federal government agencies in the United States.[42] A different vulnerability was used in another attack against several versions of Exchange Server in August 2021.[43]

MALWARE

Ransomware is a type of malware, but other types attempt to compromise devices for data theft, persistent access, and credential theft. One study found that the government sector faced the fourth largest increase in malware attacks during 2020, at 25% higher than the average attack rate—compared to 32.2% for Wholesale Trade, which was in first place.[44] In August, the station departure boards for Iran's railway system were hacked. The compromised signage displayed a warning message and directed passengers to call a number for more details—the number was the office for Iran's Supreme Leader.[45] The attack was part of a longer-running attack against the ministry of roads and the railroad system.[46]

Foreign governments, cyberactivists, and email hackers are interfering with elections and other democratic processes.

NON-MALICIOUS HUMAN ERROR

People make mistakes all the time—even in government circles—and digital channels unfortunately amplify the effects of simple mistakes with sensitive and confidential data. Incidents during 2021 included email blunders revealing private email addresses of vulnerable citizens,[47] accidental deletion of police case files during a data migration when an employee did not follow proper procedures,[48] and sensitive data on over 80,000 agency employees accessible without a password on the agency's intranet site.[49] One study found that in the previous 12 months, 84% of organizations have experienced an insider data breach caused by human error.[50]

MALICIOUS INSIDERS

Malicious actions by employees threaten the government sector, although such incidents are normally classified as espionage. Examples include supplying data to foreign governments, leaking information to the press, and making unauthorized copies of government lists and databases. During 2021, an intelligence analyst who supplied printed copies of classified information to a reporter for publication was sentenced to prison for 45 months, with 3 years of supervision after being released. Although the offending happened in 2013–2014, sentencing details were finalized more than 6 years later.[51]

ELECTION INTERFERENCE

In recent years, foreign governments, cyberactivists, and email hackers have interfered with elections and other democratic processes across the United States, the United Kingdom, and Europe, among others. Interference has included attacking the technology systems that support an election and the ballot counting process as well as social engineering to confuse citizens about the election and candidates through "fake news." Election interference is a highly political and sensitive issue for all involved because it affects the trajectory of countries, political parties, outcomes for citizens, and careers.

IMPERSONATING GOVERNMENT AGENCIES: ATTACKS ON CITIZENS

While cybercriminals often attack government agencies directly, they also leverage the official authority of government agencies as lures for unsuspecting citizens. Phishing attacks against citizens using impersonated sender details is a prime example. Recent incidents include attempts to redirect unemployment benefit payments in Colorado by using email and phone messages that masqueraded as originating from the Colorado Department of Labor and Employment,[52] and multiple COVID-themed attacks in the early days of the pandemic in 2020.[53]

The Attractiveness of Government as a Cybersecurity Target

The government sector is an attractive target for cybercriminals for a range of reasons, many of which are endemic to the industry. In this section, we look at why the government sector is an attractive target for cybercriminals.

GOVERNMENT AGENCIES CARRY SYMBOLIC MEANING FOR THE SECURITY OF A COUNTRY

Some federal and central government agencies carry symbolic meaning for citizens in the wider country, and a cybersecurity incident at any of these organizations shatters the collective sense of safety and security on the global stage. In the United States, symbolic agencies include the White House, the State Department, the Department of Defense, the Department of Homeland Security, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA). Undermining the confidence of citizens is an attractive outcome for foreign powers, nation-state attack groups, and activist cybercriminals.

Cybersecurity incidents at agencies that carry symbolic meaning for a country's security shatter the collective sense of safety among citizens.

HOLD VITAL AND CLASSIFIED DATA

Government agencies hold data that is valuable to foreign governments, other political parties, dissenters, and hackers seeking data for identity theft and targeted phishing attacks. For example:

- Agencies create and maintain sensitive data on military maneuvers, defense plans, known and suspected terrorists, deployment locations and identity details of intelligence agents in other countries, and other issues of national security and foreign policy. Unauthorized disclosure of such classified data has negative impacts on people, organizations, and nations.
- Citizens have no choice but to supply their own sensitive and confidential data to government agencies during routine interactions, such as filing tax documentation, paying local and state taxes, and applying for business licenses. By virtue of what the government does, it accumulates a massive data footprint of some of the most sensitive and confidential data related to people and organizations.

OPERATE CRITICAL INFRASTRUCTURE

Some governments operate critical infrastructure, and attacks against such installations can have devastating effects across a large proportion of constituents. City, county, and local governments often own transactions and processes which are critical to the economic wellbeing of a city, and a ransomware attack can cause mass disruption.

GOVERNMENT EMPLOYEES UNDER INTENSE WORKLOADS AND PUBLIC SCRUTINY

Employees at government entities face both intense workloads and the expectations of the wider citizenry to be perfect at all times. Mistakes in routine transactions or email messages sent to the wrong person can lead to public investigations, data breach notifications, and public attacks via news media.

CYBERSECURITY IS ONLY ONE OF MANY CRITICAL ISSUES

Responding to cybercrime and cybersecurity threats is but one of many critical issues currently facing governments. Other critical issues include national security, foreign policy considerations (for the United States—especially Russia, China, and Iran), the ongoing effects of the COVID-19 pandemic on people and supply chains, climate change, terrorism, and other regional conflicts.[54] Ensuring the right level of attention is invested in each issue relative to all the others is a perpetual challenge.

INSUFFICIENT SUPPLY OF CYBERSECURITY PROFESSIONALS

There is a global shortage of cybersecurity professionals with the right level of skills, and government agencies struggle to hire and retain top-flight talent. Private sector firms offer higher compensation than the government, and once younger associates hold Microsoft certifications, for example, they are worth more in the market than an agency can afford. Many of the current cybersecurity professionals in government are approaching retirement age, foreshadowing a massive talent shortage in the coming years.

The new Florida Digital Service—created in 2020 to hold state-level oversight of cybersecurity—has a general vacancy rate of 33%, cannot fill half of the cybersecurity response team roles, and is looking for its third Chief Information Security Officer within a year of being established.[55] Globally, there are over 4 million unfilled positions in cybersecurity,[56] which is 270% higher than the number in our Cybersecurity in Government report from 2019.[57]

Government agencies struggle to hire and retain top-flight cybersecurity talent.

INSUFFICIENT FUNDING

Cybersecurity spending should equate to about 5% to 15% of an organization's annual IT budget, in general across industries. The actual percentage should be set in reference to the types of threats and the severity of impact following a cybersecurity incident. Government agencies spending at the lower end of this range—or below—are increasingly vulnerable to cyberattack.

LEGACY SYSTEMS

Government agencies still running Windows 7, older Windows Server versions, thick client applications (e.g., enterprise resource planning systems), and other major operational systems which are no longer patched against vulnerabilities are at risk from malware and other exploits. The government sector is racing to eradicate such dependence,[58] but until these older versions are removed entirely, agencies are under threat from attacks directly against their own infrastructure, as well as from the compromise of legacy systems at a trusted partner that flows through to an agency.

LOW CYBERSECURITY READINESS

The combination of an insufficient supply of cybersecurity professionals, insufficient funding, and the presence of legacy systems quickly conflates to a position of low cybersecurity readiness. If the sector had come off the back of a massive cycle of investment in cybersecurity and this was merely a short-term blip, the outlook would be different. However, these issues have been systemic to the sector for many years, and it will take significant investment across the sector for multiple years in people, process, and technology to redress.

SMALLER CITIES AND AGENCIES, DECENTRALIZED BUDGETS, AND SECURITY OPERATIONS

Countries with hundreds or thousands of smaller cities, municipalities, counties, and agencies offer a rich tapestry of attack options to cybercriminals. Each entity holds the responsibility to protect their people and operations, along with self-determination for expenditure on security operations and hire of appropriately skilled cybersecurity professionals. Large federal, state, and local government agencies more often have the reach, budget, and personnel to deliver higher security than these smaller entities.

MOVING TO THE CLOUD WITHOUT PROPER SECURITY

Hyperconvergence on hyperscale cloud services raises security risks for public and private sector organizations alike. Moving to the cloud requires navigating issues such as lower visibility into cyberattack vectors, configuring new services with appropriate security settings, learning to manage the shared responsibility model with cloud providers, and determining the line between insufficient and "good enough" for native security services offered by a cloud provider versus using third-party solutions to bolster security. These issues require the expertise of IT cloud architects and cybersecurity professionals that is often unavailable.

Cloud services are also vulnerable to attack due to undiscovered threat pathways. In August 2021, security researchers found a way into Microsoft Azure Cosmos DB—a fully managed cloud database platform—gaining access rights for reading, writing, and deleting data in customers' Cosmos instances.[59] Government agencies using cloud services are not immune to vulnerabilities in cloud platforms.

Attacks against cloud services and supply chain partners contribute to the extensive attack surface in government.

VULNERABILITY TO ATTACKS AGAINST SUPPLY CHAIN PARTNERS

Government agencies complement the skills of government employees with contractors from other firms and use software supplied by the private sector. Attacks against people and firms in this longer supply chain of talent and capability have cascading effects on government agencies. For example, the 2020 ransomware attack at Tyler Technologies, a provider of software and IT services to government clients, resulted in suspicious logins to applications it had provided to clients.[60] Low cybersecurity preparedness at other firms, along with systemic security weaknesses in technology and practice, is exploited by cybercriminals to attack government targets.[61] In addition, across all industry sectors, the federal government faces the second highest rate of insider incidents perpetuated by trusted business partners.[62]

EXTENSIVE ATTACK SURFACE

A confluence of millions of people, devices, servers, cloud applications, and identity credentials are used within the government sector, along with tens of millions of email messages each day. The attack surface is extensive, providing many opportunities for nation-state actors, hackers, and activists to seek points of compromise.

Heightened Awareness of Cybersecurity: Governments Respond

Governments around the world are taking a more activist approach to responding to cybersecurity threats—particularly ransomware against both public and private organizations. In this section, we briefly consider recent moves by governments in the United States and elsewhere.

UNITED STATES

The Biden administration is placing increasing emphasis on developing resilience in the face of cybersecurity threats against the government and other industry sectors. Ransomware is a key concern, considering recent disruption to critical infrastructure such as the Colonial Pipeline and JBS attacks. While there is a high focus on better securing government agencies, the administration is also directing American businesses to take cyberthreats and ransomware seriously. Many of the directives parallel what is required of government agencies. Three specific initiatives from the United States government are:

- **Executive Order on Improving the Nation's Cybersecurity**
  Issued in May 2021, Executive Order 14028 mandates improved information sharing on cybersecurity between the U.S. government and the private sector, requires stronger cybersecurity standards within the federal government (e.g., widespread adoption of multi-factor authentication, encryption, and zero trust), removes current barriers for service providers to share threat intelligence, elevates the importance of security in the software supply chain (including visibility into software composition), and establishes the Cyber Safety Review Board to analyze significant cyber incidents and make recommendations, among others.[63] The administration is working with private sector organizations to improve the nation's cybersecurity readiness, has secured significant commitments from Apple, Google, Microsoft, and Amazon, and is working with others to address the cybersecurity skills shortage.[64]
- **Joint Cyber Defense Collaborative (JCDC)**
  Part of the Cybersecurity & Infrastructure Security Agency (CISA), the JCDC was created in 2021 to lead the development of cyber defense plans in the United States to safeguard critical infrastructure and national interests.[65] Its mission includes working with private and public sector organizations.
- **StopRansomware.gov**
  Multiple federal government agencies, including the Department of Homeland Security and the Department of Justice, launched a one-stop resource for combating ransomware.[66] Released in mid-July 2021, the website consolidates the ransomware resources from all federal government agencies into a single location, replacing the previous approach of resources being distributed across a variety of locations.

The Biden administration is placing increasing emphasis on developing resilience in the face of cybersecurity threats against the government and other industry sectors.

UNITED KINGDOM

Enhancing the UK's cybersecurity position is an important component of the UK's 2021 policy paper on security, defense, development and foreign policy for Britain.[67] Building resilience in the face of cyberattacks is an aspect of one of the four key objectives in the policy, and a more detailed cybersecurity strategy is due later in 2021. The UK wants to improve its global standing in the technologies essential to cyber power, and formally established the National Cyber Force as part of the UK's Ministry of Defence.

Addressing the threat of ransomware is a key issue for the government and is viewed as being more significant than dealing with nation-state threats.[68] The UK's National Cyber Security Centre has updated its guidance on mitigating malware and ransomware in the public sector and large organizations. The guidance focuses both on preparedness and response to an incident.[69]

EUROPE

A new EU Cybersecurity Strategy was presented in December 2020 with a focus on bolstering Europe's resilience against cyberthreats, strengthening cooperation with partners around the world, and assuring the physical and cyber resilience of critical entities and networks.[70] Specific proposals include establishing Security Operations Centers across the EU for early detection and rapid response to cybersecurity threats, upskilling the workforce, and solving the cybersecurity skills shortage problem. It also includes the vision of creating a Joint Cyber Unit by 2022 to respond to mass cyber incidents in an advanced and coordinated way across the Union.[71]

AUSTRALIA

An updated Cyber Security Strategy was released in August 2020, noting the continuation of rapid cyberthreat evolution. The strategy aims at improving cyber protections for the government, businesses, and critical infrastructure, commits to an investment budget over the next decade, and acknowledges that improved cybersecurity involves the collaboration of government, industry, and community members.[72] A complementary workstream is looking at enhanced protections for critical infrastructure.[73]

SINGAPORE

The current Cybersecurity Act focuses on protecting critical infrastructure in Singapore, enabling information exchange after an incident, and provides authorization for the Cyber Security Agency of Singapore to investigate incidents and threats.[74] The government recently expanded its cooperation with the United States government on cybersecurity,[75] and offers ongoing education and insight to citizens on cybersecurity threats against the country.

Governments around the world are taking an increasingly activist approach to protecting their national interests and critical infrastructure against cyberthreats.

Changing Dynamics of Cybersecurity Threats: Expectations

Ransomware attacks against government targets were the headline issue in our 2019 report on Cybersecurity in Government, and in two years this has grown into an even greater issue given the success of recent attacks. In this section, we outline our expectations for the changing dynamics of cybersecurity threats in the government sector.

RANSOMWARE AGAINST CRITICAL INFRASTRUCTURE

With all the attention governments are directing at the issue of ransomware against critical infrastructure, we expect to see ongoing efforts by cybercriminals to destabilize economic and political power through such attacks. Not all critical infrastructure is controlled directly by government, but governments have a regulatory and law-setting role to play in how a country's critical needs are met for electricity, air and ground transportation, water, telecommunications, fuel, financial services, healthcare, and more. These attacks have a direct impact on larger populations of citizens. They also offer an approach to cyber warfare between countries, similar to the systematic attacks by Russia on the Ukraine[76] and other countries.

TARGETED ATTACKS AGAINST SYMBOLIC FEDERAL AND CENTRAL GOVERNMENT AGENCIES

Federal and central government agencies carry symbolic meaning for a country or region, and a major cybersecurity incident at any of these agencies is highly distressing to the citizenry. Any agency that deals with national security interests, cybersecurity policy and implementation in government, federal or central law enforcement, or lawmaking functions is viewed as a highly desirable target. While these symbolic agencies may not be compromised, they will remain under relentless attack from all sides.

Ransomware continues to be the headline issue for governments.

LOW-HANGING FRUIT AND EASY TARGETS

The headline issue will remain ransomware for the foreseeable future, but other easy-to-operate cyberthreats will continue. Phishing campaigns, for example, continue to work even with low click rates, and email accounts compromised through phishing can be used for cascading business email compromise attacks to steal funds or divert payroll.

WEAPONIZATION OF GOVERNMENT AGENCIES TO ATTACK CITIZENS

Government agencies that are successfully compromised could be weaponized by cybercriminals to attack citizens, disrupt daily life, and undermine confidence in government. Examples include phishing attacks originating from compromised agency email accounts, incorrect payments that require significant effort by both citizens and an agency to untangle, and fabricated misdemeanor notices.

Improving Cybersecurity in Government: Solutions to Consider

The Biden administration's executive order on cybersecurity includes a range of newly mandated requirements—including more extensive adoption of multi-factor authentication, data encryption, endpoint detection and response across the government, and securing the software supply chain. We concur on their importance in the government sector. In this section, we review the basics to get right—including many from the executive order—and cover complementary areas for enhanced and added protections for government agencies who understand the need to get ahead of the curve.

MAKE A PLAN

The best place to start for improving cybersecurity is to make a plan. Every government entity needs a plan for cybersecurity, including:

- **Risk assessment**
  What types of threats are currently being experienced and which threats are likely to be experienced in the future? We have explored many of these risks and threats earlier in this paper, although there may be other critical cybersecurity threats to include. Different government entities are susceptible to a different mixture of threat types. Improved threat intelligence sharing within the government sector, including leveraging threat data from Information Sharing and Analysis Centers (ISACs) around the world, will also elevate awareness of emerging sector-wide threats.
- **Security policy development and configuration**
  Based on your risk assessment and understanding of the people gaining access to your systems, develop granular security policies that apply the correct amount of security for the quantum of cyber risk presented. This ensures security is maintained and provides greater usability and convenience to users and data that does not require as much protection. Granular security policies are also a key element and success criteria for implementing zero trust.
- **Incident response plan**
  Given the frequency of attack attempts, develop a plan for how to respond to a successful cyberattack and recover in the case of a significant compromise. Developing the organizational protocols for response and recovery before being compromised is essential because it enables preparation, analysis, and decision-making without the urgency and stress of also dealing with a current incident.

The best place to start for improving cybersecurity is to make a plan: assess your risks, develop a security policy, and know how you will respond to an incident.

Improving cybersecurity does not happen overnight; it requires careful planning and a roadmap to implement.

STRENGTHEN IDENTITY AND AUTHENTICATION

Stop relying on usernames and passwords for proving identity and gaining access to sensitive, confidential, secret, and other personal data. A username/password combination is susceptible to a phishing attack, password spraying, and brute-force attacks, among others, and once compromised provides access to whomever holds the combination. The devastating compromise at the U.S. Office of Personnel Management in 2015 was traced back to stolen credentials.[77] Stronger and less vulnerable approaches to identity and authentication are essential, including:

- **Single sign-on**
  Single sign-on enables a significant reduction in the number of credentials required to access systems, streamlines user adoption, simplifies credential revocation when an employee leaves, offers a unified identity for reporting, and facilitates adding stronger security protections to a single credential because it must be completed less frequently. Optimize single sign-on by connecting all applications, especially thick client apps and legacy systems, to remove isolated passwords and eliminate all weak links.

- **Strong multi-factor authentication**
  Osterman Research has advocated the use of MFA for many years, and with MFA included in the list of core protections from the Biden administration, we are not about to withdraw our standing recommendation. However, we note that not all MFA solutions are created equal, and we strongly advise the use of MFA solutions with stronger protections. Wherever possible, MFA that relies on biometrics and public-key cryptography should be used rather than MFA approaches that rely on SMS codes and email notifications. In government use cases where the highest level of identity verification is needed, biometrics offer the only way to positively identify an individual rather than a device or token. Authenticator app–based MFA is also positioned towards the stronger end of the MFA continuum. Users are likely to require flexible options for MFA to counteract variations in device capabilities, forgotten tokens or phones ("I left it at home"), and cell coverage dead spots if SMS codes are used, despite our recommendation against them. Organizations not using MFA are only asking for trouble, but equally, so too are organizations that blindly implement MFA with false hope in its efficacy.

- **Passwordless authentication and biometrics**
  Wherever possible, move toward passwordless authentication using biometrics and public-key cryptography for proving identity and gaining access to systems; these are much stronger and more convenient than legacy authentication approaches. Where passwords must still be used, complex and unique passwords are strongly recommended rather than reusing passwords across applications.

- **Risk-based authentication**
  Rather than merely attempting to match a credential combination, modern authentication systems assess the risk attributes or context of an authentication request and allow, deny, or only partially allow login attempts based on the level of risk. For example, requests with higher risk attributes could include attempts from foreign countries from unmanaged devices or untrusted networks, and behavior outside of the user's regular login patterns. Alternatively, requests with lower risk attributes could include authentication attempts from within the network, from a managed device, occurring within regular business hours, and in accordance with the baseline login patterns of the user.

Use stronger approaches to identity and authentication, such as single sign-on, strong MFA, and biometrics.

- **Unified identities for citizens**
  Offering a unified identity service for citizens when interacting with government services and systems provides a single version of the truth rather than a disjointed set of identities. Unified identities for citizens enable stronger protections to be enforced for logins and reduces the number of disparate credentials that citizens have to remember, manage, and protect.

PROTECT DATA WHERE IT RESIDES

Every system holding government data must be protected from unauthorized access, modification, and deletion. Databases, cloud storage accounts, file servers, and email accounts should be continuously monitored for baseline protection settings and configuration drift. Information governance solutions enable the discovery and identification of sensitive data wherever it is stored (so protections can be put in place), Cloud Access Security Broker (CASB) solutions monitor the use of cloud services and enforce configuration settings (among other capabilities) and encrypting data with strong public-key cryptography is almost 100% guaranteed to prevent usable data from being exposed after a data breach.

PROTECTED BACKUPS

Protect backups from both unauthorized access and ransomware infiltration. Having up-to-date backups available is the easiest, most reliable, and least costly approach to recovering after a ransomware incident, but this only works if the ransomware attack has not also compromised backup data. Cybercriminal gangs have been known to supply a decryption key that does not decrypt all data—with average rates of recovery pegged at 65% in one large study.[78] In other words, even if the ransom demand is paid, organizations risk losing one third of their data. Protected backups in combination with end-to-end encryption of sensitive, confidential, and secret data greatly reduces the threat of multi-level ransomware extortions.

STRENGTHEN METHODS OF SHARING DATA TO PROTECT DATA IN MOTION

Email is currently the most common way of sharing documents and files within agencies, across agency lines, and outside of the government sector. Documents containing sensitive and personal data sent by email should be protected with additional protection using encryption. This reduces the likelihood of a data breach if the message is sent to the wrong person, and also if the email account is compromised.

Managed file transfer solutions offer a much stronger foundation for sharing and protecting sensitive data. Transferred files are protected by encryption, access is controlled through identity verification, and files are never stored in email accounts.

Managed file transfer solutions offer a much stronger foundation for sharing and protecting sensitive data in government compared to using email messages with attachments.

DEFEND AGAINST PHISHING

General and targeted phishing campaigns are the primary attack vector for credential theft, financial compromise, ransomware attacks, data breaches, and more. As noted in the previous section, we expect to see ongoing use of phishing against the government sector.

Strengthen phishing defenses through anti-phishing solutions, including:

- **Email authentication**
  Strengthen email authentication by implementing the DNS triple therapy of SPF, DKIM and DMARC. These three protections work in combination to reduce the ability for unauthorized messages to be sent and received, protecting both the organization and its constituents.
- **Known threats**
  Scan messages and attachments for known threats, indicators of malicious intent, and spam signals.
- **Internal phishing**
  Watch out for internal phishing. Email messages from known and trusted internal email accounts can used for delivering malicious payloads or in BEC attacks when the email account has been compromised by a threat actor.
- **Advanced threat protection**
  New threat methods are constantly being developed by cybercriminals to evade signature-based detection mechanisms. Advanced threat protection solutions look beyond known indicators of threat for unusual behavior in an attachment, recursively check messages and attachments to uncover hidden threats, and assess the veracity of links each time they are clicked to mitigate the threat of post-delivery weaponization.
- **Contextual changes also helpful**
  Complementary contextual changes have cascading effects on phishing, such as implementing strong MFA, reducing human susceptibility to social engineering phishing attacks through security awareness training, and establishing checks and balances outside of email for authorizing financial transactions, changing bank routing details, and updating vendor records.

ENHANCE OPTICS AND VISIBILITY

Visibility into the current state and security posture of endpoints, cloud services, applications, and commercial software provides the ability to mitigate identified threats before they can be used in an attack. Enhancing optics and visibility into areas of vulnerability includes:

- **Automated scanning and patching**
  Automated scanning for known and newly identified vulnerabilities across devices and systems, combined with automated and virtual patching. Rapidly identifying and patching vulnerabilities eliminates attack opportunities.
- **Protect cloud services**
  Not being blindsided by a data breach on an unknown or insufficiently secured cloud service. A Cloud Access Security Broker (CASB) can discover cloud services being used by looking at network and device traffic and enable automated policy-based remediation. CASBs can also ensure that security configuration settings on cloud services remain intact and correct.
- **Software supply chain**
  Knowing the security standing of your software supply chain, both by reference to published software bills of materials (SBoMs) and by code analysis on internally developed and commercially acquired software products. Code analysis solutions highlight coding weaknesses, uncover unknown vulnerabilities, and identify known vulnerabilities in open-source components included surreptitiously in commercial software.

Enhance visibility into areas of vulnerability, including automated scanning and patching, code analysis on software, and endpoint detection and response.

- **Endpoint/extended detection and response (EDR and XDR)**
  Endpoint Detection and Response (EDR) solutions focus on quickly detecting indicators of compromise via malware, malicious attachments, and other threats on endpoints. EDR solutions can be used to understand the threat surface across all endpoints and remediate newly identified weaknesses. Extended Detection and Response (XDR) solutions increase the remit beyond endpoints only, encompassing threat signals and correlations across email, servers, cloud workloads, and network traffic as well.

THREAT INTELLIGENCE MANAGEMENT PLATFORMS

Threat intelligence management platforms ingest data on security incidents, emerging campaigns, and from multiple shared threat intelligence sources to aggregate threat signals, curate disparate data, and correlate common threat indicators. Threat intelligence platforms automatically update security protections across the organization's suite of security tools—such as the firewall, EDR/XDR, and intrusion protection—to ensure new security safeguards are immediately applied. By automatically addressing new and emerging security incidents, threat intelligence management platforms help to mitigate the cybersecurity skills shortage. Workflow capabilities enable coordination with Security Operations Center (SOC) analysts, and reporting tools are offered to keep management apprised of current threats.

SECURITY AWARENESS TRAINING AND TESTING

People unaware of security threats will fall for them.

People lacking awareness of organizational processes for reporting cybersecurity threats will not use them.

Security awareness training—and the integral testing component of modern training—mitigates both challenges. The intent is to increase cybersecurity maturity, awareness, and competence among staff, employees, managers, executives, and government officials. Aspects of security awareness training includes:

Use security awareness training and testing to increase cybersecurity maturity, awareness, and competence.

- **Training campaigns**
  Training campaigns to inform and educate that are delivered regularly and repeatedly in formats that can be consumed by people in the office and beyond. For example, modern security awareness training uses posters, video case studies, and content for email campaigns to strengthen the human line of defense against phishing, BEC, data breaches, privacy invasions, and more.
- **Testing and assessment**
  The testing side of security awareness training provides an ongoing mechanism for ascertaining the efficacy of training, along with the likelihood that attacks will be successful. Where testing shows that training has been ineffective, mitigations can be planned—often in the form of further training or coaching, and sometimes in the form of technology mitigations such as browser isolation.
- **Organizational processes**
  Design of organizational processes for reporting suspected threats, getting a second opinion on a realistic-looking but out-of-the-ordinary request, and raising the alarm on an actual incident.

CLOUD SECURITY SERVICES

Cloud-based security services are available to protect email, web applications, cloud workloads, and identities, among others. Cloud services replace the need for on-premises deployments at each government entity and simplify configuration and ongoing management. The use of cloud security services contributes to mitigating the shortage of cybersecurity professionals, offers threat signals from a wider population of government and civilian organizations, and may include access to highly trained threat experts.

CYBERSECURITY INSURANCE

A cybersecurity insurance policy provides financial coverage for worst-case situations, enabling an agency with no other way of recovery to return to an operational state. However, there are additional benefits from securing such coverage, such as being subjected to a third-party review of current cybersecurity protections that offers best-practice insight into current systemic weaknesses at your organization. Insurers are likely to require the types of security controls mentioned in this report, such as MFA.[79] Some insurance providers also have cybersecurity talent available to assist with recovery after an incident.

The disadvantage of cybersecurity insurance is that recovering data by paying the ransom does nothing to enhance the preparedness of the organization to counteract future attacks. Having cybersecurity insurance can offer a recovery method of last resort, but unless systems are hardened, people are better trained, and processes developed, one successful cybersecurity incident against an organization that is settled by an insurance company increases the likelihood of being attacked again. Some ransomware gangs search for cybersecurity insurance policy documents immediately after an initial compromise and use what they learn in setting the ransom demand.[80] Finally, as government officials repeat often, paying the ransom demand merely funds and encourages further ransomware attacks.

Cybersecurity insurance can fund a ransom payment but cannot harden systems against future attacks.

ADDRESS THE CYBERSECURITY SKILLS GAP

Government agencies and organizations alike need bodies on the ground to spearhead cybersecurity strategy, preparations, and response. Technology cannot do it alone. Look for partnership opportunities with colleges and universities to train the next generation of cybersecurity professionals, along with vendors and consultants who can add or augment internal cybersecurity expertise.

Conclusion

The government sector continues to face severe cybersecurity threats, with the broader threat against critical infrastructure from ransomware as the issue that is gaining the most attention in government circles. There is a need to protect the wider economy and society from the threat of ransomware and other cyberattacks, which means the government sector itself must continue to improve its own cybersecurity readiness, preparedness, and defenses. We recommend carefully evaluating the threats against government entities, developing a strong cybersecurity plan in response, and investing in the cybersecurity solutions and best practices profiled in this white paper.

Sponsors of This White Paper

ANOMALI

Anomali is the leader in intelligence-driven extended detection and response (XDR) cybersecurity solutions. Anchored by big data management and refined by artificial intelligence, the Anomali XDR platform delivers proprietary capabilities that correlate the largest repository of global intelligence with telemetry from customer-deployed security solutions, empowering security operations teams to detect threats with precision, optimize response, achieve resiliency, and stop attackers and breaches. Our SaaS-based solutions easily integrate into existing security tech stacks through native cloud, multi-cloud, on-premises, and hybrid deployments. Founded in 2013, Anomali serves public and private sector organizations, ISACs, MSSPs, and Global 1000 customers around the world in every major industry. Leading venture firms including General Catalyst, Google Ventures, and IVP back Anomali.

Learn more at www.anomali.com.

ANOMALI

www.anomali.com

@Anomali

general@anomali.com

+1 844 4 THREATS (847328)

+44 8000 148096
(International Toll-Free)

808 Winslow Street
Redwood City, CA 94063

BIO-KEY INTERNATIONAL

BIO-key is a trusted provider of Identity and Access Management (IAM) and Identity-Bound Biometric solutions that offer an easy and secure way to authenticate the identity of employees, customers, and suppliers while managing their access across devices and applications.

Over 1,000 global customers, including the federal government and 200+ higher education institutions trust BIO-key PortalGuard IDaaS, an award-winning IAM platform, to reduce password-related help desk calls by up to 95%, eliminate passwords, secure remote access, prevent phishing attacks, and improve productivity for the IT team. PortalGuard provides the simplicity and flexibility required to secure the modern digital experience with options for single sign-on, self-service password reset, and over 16 multi-factor authentication methods, and is the only IAM platform to offer Identity-Bound Biometrics.

Backed by decades of expertise, BIO-key has a proven track record of successful IAM project delivery and strong customer relationships.

More information is available at www.BIO-key.com.

BIO-key®

www.BIO-key.com

info@BIO-key.com

+1 732 359 1100

KNOWBE4

KnowBe4 is the provider of the world's largest security awareness training and simulated phishing platform. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security. Kevin Mitnick, an internationally recognized cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organizations rely on KnowBe4 to mobilize their end users as the last line of defense.

To learn more, please visit www.knowbe4.com.

KnowBe4
Human error. Conquered.

www.knowbe4.com

@KnowBe4

info@knowbe4.com

+1 855 566 9234

MIMECAST

Mimecast helps over 850 government organizations and educational institutions protect their employees, intellectual property, customer data, and brand reputations by providing comprehensive cloud-based security and compliance solutions that mitigate risk and reduce the cost and complexity of creating a cyber-resilient organization. Our Email Security Solution is backed by over a decade of continuous enhancement and practical application, garnering Mimecast the trust of tens of thousands of customers and millions of users globally.

In an era where attacks are becoming increasingly sophisticated, a defensive strategy that addresses viruses and spam alone is no longer enough. From spear-phishing attacks to email-borne ransomware, the threat landscape isn't what it was yesterday—nor will it be the same tomorrow. Mimecast's Secure Email Gateway with Targeted Threat Protection is designed to help you mount the best possible defense for whatever comes your way, providing a secure email gateway in the cloud, which applies a dynamic, multi-layered approach to the analysis of inbound, outbound, and internal emails. From higher-level inspections such as DNS authentication, including SPF/DKIM/DMARC and spam/virus protection, to highly sophisticated checks like static file analysis and sandboxing, this comprehensive service goes well beyond just cloud-based anti-virus and anti-spam protections.

Mimecast's email security protection services can be expanded and enhanced with a number of solutions designed to increase resilience, protect company data, ensure continuity and support rapid recovery in the face of an attack, and more. All these solutions are fully integrated with Mimecast's core email security service to seamlessly deliver comprehensive protection.

Mimecast is here to help protect large and small organizations from malicious activity, human error, and technology failure, and to lead the movement toward building a more resilient world.

Learn more about us at www.mimecast.com.

www.mimecast.com

@mimecast

UK/EUROPE
+44 (0) 207 847 8700
info@mimecast.com

NORTH AMERICA
+1 800 660 1194
+1 781 996 5340
info@mimecast.com

SOUTH AFRICA
+27 (0) 117 223 700
0861 114 063
info@mimecast.co.za

AUSTRALIA
+61 3 9017 5101
1300 307 318
info@mimecast.co.au

PROGRESS MOVEIT

Progress MOVEit is the leading secure managed file transfer application used by thousands of organizations worldwide to provide complete visibility and control of file transfer activities. MOVEit enables the secure transfer of sensitive data with advanced collaboration and workflow automation capabilities, all without the need for scripting. MOVEit extends file transfer capabilities to all users to eliminate insecure use of email and quickly onboard partners and third parties. Accelerate your business and effortlessly create automated file transfer tasks and workflows to eliminate the risk of user error. MOVEit makes it easy for your users to safely transfer data, collaborate and scale to support your business needs – all while minimizing the burden on IT.

Learn more at www.ipswitch.com/moveit.

www.ipswitch.com/moveit

@ProgressMOVEit

+1 800 477 6473

VIRSEC

Virsec is the world's leading provider of application-aware workload cyber protection. Virsec's unique technology defends against the widest range of attacks, both known and unknown, with no signature or prior knowledge required. The solution secures any and all critical business applications, from legacy to commercial off-the-shelf software (COTS) to custom, in any environment. Virsec is led by industry veterans with extensive leadership experience at multiple leading cybersecurity and technology companies and a long list of high-growth startups.

More information is available at www.virsec.com.

www.virsec.com

info@virsec.com

[1] Osterman Research, How to Reduce the Risk of Phishing and Ransomware, March 2021, at https://ostermanresearch.com/2021/03/17/orwp_0336/
[2] AtlasVPN, Ransomware attacks surge by over 150% in 2021, August 2021, at https://atlasvpn.com/blog/ransomware-attacks-surge-by-over-150-in-2021
[3] The Maine Monitor, In a first for Maine, ransomware hackers hit 2 public wastewater plants, August 2021, at https://bangordailynews.com/2021/08/15/news/in-a-first-for-maine-ransomware-hackers-hit-2-public-wastewater-plants/
[4] Jacob Bunge, JBS Paid $11 Million to Resolve Ransomware Attack, June 2021, at https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781
[5] Jessica Davis, Health sector deals with ransomware, data breaches as COVID cases rise, August 2021, at https://www.scmagazine.com/analysis/breach/health-sector-deals-with-ransomware-data-breaches-as-covid-cases-rise
[6] Paul Reynolds, Gardai Not Aware of Any Stolen HSE Data Published Online, May 2021, at https://www.rte.ie/news/health/2021/0524/1223542-cyber-attack/
[7] Thomas Manch and Libby Wilson, Waikato DHB Scrambles to Contain Cyber Attack, Safety of Patient Data Unclear, May 2021, at https://www.stuff.co.nz/national/health/125235676/waikato-dhb-scrambles-to-contain-cyber-attack-safety-of-patient-data-unclear
[8] The National Herald, Cyberattack Shuts Down Services in Greece's Second-Largest City, July 2021, at https://www.thenationalherald.com/archive_general_news_greece/arthro/cyberattack_shuts_down_services_in_greece_s_second_largest_city-2960445/
[9] Sophos, The State of Ransomware in Government 2021, June 2021, at https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-state-of-ransomware-in-government-2021-wp.pdf
[10] John Sharp, Mobile County Cyberattack Shut Down Systems for 3 Days, Sparked Federal Investigation, June 2021, at https://www.al.com/news/2021/06/mobile-county-cyberattack-shut-down-systems-for-3-days-sparked-federal-investigation.html
[11] Illinois Attorney General, Important Notice from the Illinois Attorney General Regarding Computer Network Compromise, April 2021, at https://illinoisattorneygeneral.gov/consumers/publicnotice/OAG_Network_Compromise_Public_Notice.pdf
[12] Jeff Arnold, Illinois AG Raoul Spends $2.5M on Ransomware Hack: Report, July 2021, at https://patch.com/illinois/chicago/illinois-ag-raoul-invests-2-5m-after-ransomware-hack-report
[13] Debby Woodin, Ransomware Shuts Down Online Services in Joplin, Mo., August 2021, at https://www.govtech.com/security/ransomware-shuts-down-online-services-in-joplin-mo
[14] Thomas Brewster, Ransomware Hackers Claim to Leak 250GB of Washington, D.C., Police Data After Cops Don't Pay $4 Million Ransom, May 202105, at https://www.forbes.com/sites/thomasbrewster/2021/05/13/ransomware-hackers-claim-to-leak-250gb-of-washington-dc-police-data-after-cops-dont-pay-4-million-ransom/
[15] Mariam Baksh, Report: Mobile Phishing to Steal Government Credentials Increased 67% in 2020, February 2021, at https://www.nextgov.com/cybersecurity/2021/02/report-mobile-phishing-steal-government-credentials-increased-67-2020/172274/
[16] Binayak Dasgupta, Phishing attack targets Indian officials through rogue email from government ID, February 2021, at https://www.hindustantimes.com/india-news/phishing-attack-targets-officials-through-rogue-mail-from-government-id-101613605003186.html
[17] Raphael Satter and Kanishka Singh, Microsoft says group behind SolarWinds hack now targeting government agencies, NGOs, Reuters, May 2021, at https://www.reuters.com/technology/microsoft-says-group-behind-solarwinds-hack-now-targetting-government-agencies-2021-05-28/
[18] GRC World Forums, Californian government agency breached in phishing attack, March 2021, at https://www.grcworldforums.com/security/californian-government-agency-breached-in-phishing-attack/1095.article
[19] Vera Bergengruen and W.J. Hennigan, The Capitol Attack Was the Most Documented Crime in History. Will That Ensure Justice?, April 2021, at https://time.com/5953486/january-capitol-attack-investigation/
[20] Department of Homeland Security, Fusion Centers, September 2019, at https://www.dhs.gov/fusion-centers
[21] KnowBe4, Multi-Factor Authentication Basics and How MFA Can Be Hacked, March 2021, at https://www.knowbe4.com/how-to-hack-multi-factor-authentication

[22] Michael Kan, Google: Phishing Attacks That Can Beat Two-Factor Are on the Rise, March 2019, at https://au.pcmag.com/google-titan-security-key-bundle/61059/google-phishing-attacks-that-can-beat-two-factor-are-on-the-rise
[23] FBI, FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics, March 2021, at https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics
[24] FBI, Private Industry Notification: Business Email Compromise Actors Targeting State, Local, Tribal, and Territorial Governments, Straining Resources, March 2021, at https://www.ic3.gov/Media/News/2021/210318.pdf
[25] GCN Staff, Report: Phishing behind 70% of government breaches, May 2021, at https://gcn.com/articles/2021/05/17/verizon-breach-report.aspx
[26] Lawrence Mower, Florida's unemployment site hacked, exposing personal data on 58,000 claimants, July 2021, at https://www.tampabay.com/news/florida-politics/2021/07/23/floridas-unemployment-site-hacked-exposing-personal-data-on-58000-claimants/
[27] GRC World Forums, Californian government agency breached in phishing attack, March 2021, at https://www.grcworldforums.com/security/californian-government-agency-breached-in-phishing-attack/1095.article
[28] Eirian Jane Prosser, Oxford City Council apologies for potential data breach, July 2021, at https://www.oxfordmail.co.uk/news/19458894.oxford-city-council-apologises-potential-data-breach/
[29] Frances Robles and Nicole Perlroth, 'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town, February 2021, at https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html
[30] Anna Ribeiro, Verizon, Bay Area water plant hacked due to compromises in Pulse Connect Secure appliances, June 2021, at https://industrialcyber.co/article/verizon-bay-area-water-plant-hacked-due-to-compromises-in-pulse-connect-secure-appliances/
[31] WizCase, Over 80 US Municipalities' Sensitive Information, Including Resident's Personal Data, Left Vulnerable in Massive Data Breach, July 2021, at https://www.wizcase.com/blog/us-municipality-breach-report/
[32] Ax Sharma, Secret terrorist watchlist with 2 million records exposed online, August 2021, at https://www.bleepingcomputer.com/news/security/secret-terrorist-watchlist-with-2-million-records-exposed-online/
[33] Shari Rudavsky, Cyber Company Swipes Data From 750K Indiana Residents, August 2021, at https://www.govtech.com/security/cyber-company-swipes-data-from-750k-indiana-residents
[34] Department of Justice, Department of Justice Statement on Solarwinds Update, January 2021, at https://www.justice.gov/opa/pr/department-justice-statement-solarwinds-update
[35] Alan Suderman, AP Sources: SolarWinds Hack Got Emails of Top DHS Officials, March 2021, at https://apnews.com/article/solarwinds-hack-email-top-dhs-officials-8bcd4a4eb3be1f8f98244766bae70395
[36] Raphael Satter and Kanishka Singh, Microsoft says group behind SolarWinds hack now targeting government agencies, NGOs, Reuters, May 2021, at https://www.reuters.com/technology/microsoft-says-group-behind-solarwinds-hack-now-targetting-government-agencies-2021-05-28/
[37] Catalin Cimpanu, DOJ says SolarWinds hack impacted 27 US attorneys' offices, July 2021, at https://therecord.media/doj-says-solarwinds-hack-impacted-27-state-attorneys-offices/
[38] Raphael Satter, Up to 1,500 businesses affected by ransomware attack, U.S. firm's CEO says, Reuters, July 2021, at https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/
[39] Krebs on Security, At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software, March 2021, at https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/
[40] Reuters, Norway's parliament hit by new hack attack, March 2021, at https://www.reuters.com/world/europe/norways-parliament-hit-by-new-hack-attack-2021-03-10/
[41] European Banking Authority, Cyber-attack on the European Banking Authority, March 2021, at https://www.eba.europa.eu/cyber-attack-european-banking-authority
[42] CISA, Emergency Directive 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities, March 2021, at https://cyber.dhs.gov/ed/21-02/
[43] CISA, Urgent: Protect Against Active Exploitation of ProxyShell Vulnerabilities, August 2021, at https://us-cert.cisa.gov/ncas/current-activity/2021/08/21/urgent-protect-against-active-exploitation-proxyshell
[44] Open Text, 2021 Webroot BrightCloud Threat Report, July 2021, at https://mypage.webroot.com/rs/557-FSI-195/images/2021-webroot-brightcloud-threat-report.pdf

[45] Graham Cluley, Indra hacking group blamed for attack on Iranian railway system that trolled country's supreme leader, August 2021, at https://grahamcluley.com/indra-hacking-group-blamed-for-attack-on-iranian-railway-system-that-trolled-countrys-supreme-leader/
[46] Iran International, Hackers Penetrated Iran's Railroad Computers Long Before July Attack, July 2021, at https://iranintl.com/en/iran-in-brief/hackers-penetrated-irans-railroad-computers-long-july-attack
[47] Daniel Smith, Work and Income privacy breach due to email mistake, August 2021, at https://www.stuff.co.nz/business/126016164/work-and-income-privacy-breach-due-to-email-mistake
[48] John Creuzot, Disclosure Regarding Missing Data from Dallas Police Department's Network Drive, August 2021, at https://www.dallascounty.org/Assets/uploads/docs/district-attorney/policies/Memo%20re%20DPD%20Data%20Loss.pdf
[49] State of North Carolina, Notice of Potential Security Problem Involving Personal Data, August 2021, at https://oshr.nc.gov/media/4084/open
[50] BusinessWire, 94% Of Organizations Have Suffered Insider Data Breaches, Egress Research Reveals, July 2021, at https://www.businesswire.com/news/home/20210713005123/en/94-Of-Organizations-Have-Suffered-Insider-Data-Breaches-Egress-Research-Reveals
[51] Department of Justice, Former Intelligence Analyst Sentenced to 45 Months in Prison for Disclosing Classified Information to Reporter, July 2021, at https://www.justice.gov/opa/pr/former-intelligence-analyst-sentenced-45-months-prison-disclosing-classified-information
[52] Aldo Svaldi, Hackers Search for New Ways to Divert Colorado UI Checks, June 2021, at https://www.govtech.com/security/hackers-search-for-new-ways-to-divert-colorado-ui-checks
[53] Bradley Barth, Phishing Emails Impersonate White House, Trump, Give False COVID-19 Guidance, April 2020, at https://www.scmagazine.com/home/security-news/news-archive/coronavirus/phishing-emails-impersonate-white-house-give-false-covid-19-guidance/
[54] Office of the Director of National Intelligence, Annual Threat Assessment of the US Intelligence Community 2021, April 2021, at https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf
[55] Lawrence Mower, As Threats Grow, Florida Lacks Cybersecurity Experts, August 2021, at https://www.govtech.com/security/as-threats-grow-florida-lacks-cybersecurity-experts
[56] Kyle Wiggers, Studies show cybersecurity skills gap is widening as the cost of breaches rises, July 2021, at https://venturebeat.com/2021/07/28/studies-show-cybersecurity-skills-gap-is-widening-as-the-cost-of-breaches-rises/
[57] Osterman Research, Cybersecurity in Government, December 2019, at https://ostermanresearch.com/2019/12/17/orwp_0317/
[58] Andrew Eversden, Are federal agencies prepared for the end of free Windows 7 support?, August 2019, at https://www.federaltimes.com/it-networks/2019/08/14/are-federal-agencies-prepared-for-the-end-of-free-windows-7-support/
[59] Wiz Research Team, Critical Vulnerability in Microsoft Azure Cosmos DB, August 2021, at https://chaosdb.wiz.io
[60] Joe Panettieri, Tyler Technologies Ransomware Attack: $1.5M in Lost Revenue, November 2020, at https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/tyler-technologies-recovery-details/
[61] Graphus, Government contractors are prime targets for phishing attacks, January 2020, at https://www.graphus.ai/blog/government-contractors-are-prime-targets-for-phishing-attacks/
[62] Daniel Costa, Patterns and Trends in Insider Threats Across Industry Sectors (Part 9 of 9: Insider Threats Across Industry Sectors), August 2019, at https://insights.sei.cmu.edu/blog/patterns-and-trends-in-insider-threats-across-industry-sectors-part-9-of-9-insider-threats-across-industry-sectors/
[63] The White House, Executive Order on Improving the Nation's Cybersecurity, May 2021, at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[64] The White House, FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation’s Cybersecurity, August 2021, at https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/
[65] CISA, Joint Cyber Defense Collaborative, 2021, at https://www.cisa.gov/jcdc
[66] Department of Homeland Security, United States Government Launches First One-Stop Ransomware Resource at StopRansomware.gov, July 2021, at https://www.dhs.gov/news/2021/07/14/united-states-government-launches-first-one-stop-ransomware-resource

[67] United Kingdom Cabinet Office, Policy paper: Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy, March 2021, at https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy
[68] Claudia Glover, Ransomware is the biggest cyber threat to the UK – and the government could do more to help, June 2021, at https://techmonitor.ai/technology/cybersecurity/uk-government-ransomware-lindy-cameron
[69] National Cyber Security Centre, Mitigating malware and ransomware attacks, March 2021, at https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
[70] European Commission, New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilience, December 2020, at https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391
[71] European Commission, EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents, June 2021, at https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3088
[72] Australian Government Department of Home Affairs, Australia's Cyber Security Strategy 2020, August 2020, at https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/australia's-cyber-security-strategy-2020
[73] Australian Government Department of Home Affairs, Protecting Critical Infrastructure and Systems of National Significance, December 2020, at https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems
[74] Cyber Security Agency of Singapore, Cybersecurity Act, March 2018, at https://www.csa.gov.sg/Legislation/Cybersecurity-Act
[75] Cyber Security Agency of Singapore, Singapore and United States Expand Existing Cooperation on Cybersecurity, August 2021, at https://www.csa.gov.sg/News/Press-Releases/singapore-and-united-states-expand-existing-cooperation-on-cybersecurity
[76] Wikipedia, Ukraine power grid hack in December 2015, August 2021, at https://en.wikipedia.org/wiki/Ukraine_power_grid_hack
[77] Alper Kerman, Zero Trust Cybersecurity: 'Never Trust, Always Verify', October 2020, at https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify
[78] Sophos, The State of Ransomware in Government 2021, June 2021, at https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-state-of-ransomware-in-government-2021-wp.pdf
[79] Kelly Paletta, Multi-Factor Authentication is Now Mandatory for Cyber Insurance, June 2021, at https://www.exptechnical.com/2021/06/07/multi-factor-authentication-required/
[80] Lawrence Abrams, Conti ransomware prioritizes revenue and cyberinsurance data theft, August 2021, at https://www.bleepingcomputer.com/news/security/conti-ransomware-prioritizes-revenue-and-cyberinsurance-data-theft/