Osterman Research
SURVEY REPORT

Survey by Osterman Research
Published **October 2020**
Sponsored by **Anomali**

Government Cybersecurity Decision Makers Index: How the Pandemic and Elections Have Focused Priorities and Shifted Concerns Across Federal, State and Local Agencies

Executive Summary

Osterman Research conducted a survey on behalf of Anomali during October 2020. We surveyed 297 CISOs, IT directors and security directors (the only roles that were permitted to participate) in US federal and state government agencies. The surveys were conducted online between October 7 and 14, 2020.

This report presents the results of that research.

KEY TAKEAWAYS

- **Massive shift to "work-from-home" operations**
  Prior to the pandemic, 11 percent of government employees were working from home. By October 2020, that number jumped to 65 percent, a 491 percent increase. This has led to security and IT decision makers now being very concerned about not having the right solutions in place to secure data and other assets, and employees working in insecure environments.

- **Misinformation is the biggest single concern**
  Prior to the pandemic, only three percent of security and IT decision makers saw misinformation campaigns as their most serious threat. As of October 2020, 17 percent (a 467 percent increase) said it had become their chief concern. This is likely due to the pandemic and an election cycle taking place at the same time.

- **Threats, attacks and breaches have increased significantly**
  Threats and attacks have increased during the pandemic compared to 2019: research findings show that threats and attacks during a typical month have jumped by 40 percent. Even worse, breaches have increased by 61 percent compared to 2019 levels.

- **Security is now a higher priority**
  The pandemic, and the security issues it has brought about, have motivated security and IT decision makers to focus more heavily on technology solutions to address the more serious threat landscape that they face. In particular, decision makers view technologies like fraud detection/prevention, vulnerability management, secure web gateways, SIEMs, and threat intelligence as much more important now than they were before the pandemic began.

- **Most are concerned about election disruptions**
  The vast majority of security and IT decision makers are concerned that bad actors may disrupt their state's 2020 presidential election operations, and many are "very" or "extremely" concerned about this eventuality. These decision makers expect Russia to be the most likely culprit behind these activities, with China running a close second. Despite a recent announcement that Iran was behind an influence campaign, the country didn't rank high as a suspected threat.

The vast majority of security and IT decision makers are concerned that bad actors may disrupt their state's 2020 presidential election operations.

ABOUT THIS SURVEY REPORT

This survey and report were sponsored by Anomali; information about the company is provided at the end of this report.

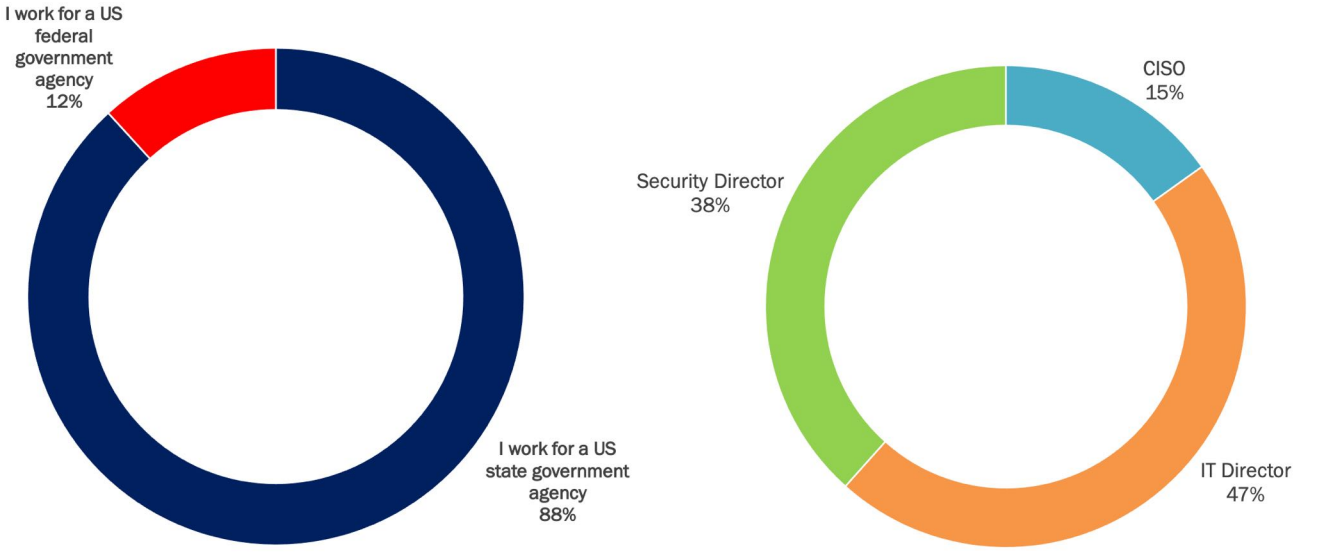
Survey Findings

SURVEY DISTRIBUTION

The survey focused on government agencies in the United States. As shown in Figure 1, the majority of organizations we surveyed are state agencies of various types and sizes. These agencies average 1,130 employees and 1,093 email users, putting them on par with small enterprise organizations.

Figure 1 also shows the distribution of roles we surveyed. Fifteen percent are CISOs, 47 percent are IT directors, and 38 percent are security directors.

Figure 1
Distribution of Survey Respondents

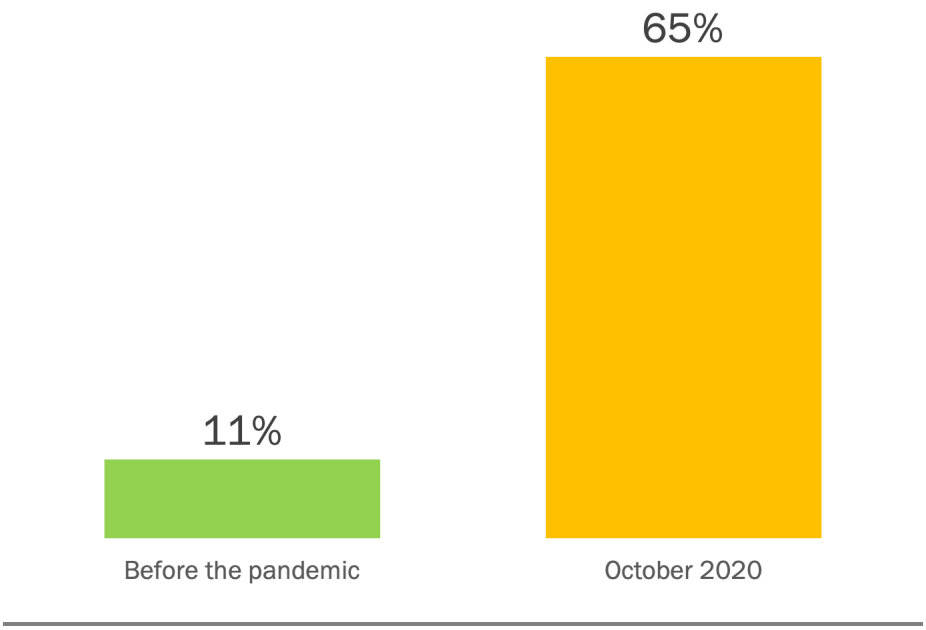


Source: Osterman Research, Inc.

WORK-FROM-HOME HAS INCREASED DRAMATICALLY

The COVID-19 pandemic and the ensuing lockdowns have had an enormous impact on the workforce and where they work. The governmental responses to the pandemic - including "social distancing", "stay-at-home" orders and "shelter-in-place" orders - have forced governments to shut down their normal operations and, where possible, enable employees to work from their homes. Those employees that are able to do so continue operating as normally as possible, albeit with numerous changes to the tools and processes to which they were accustomed - and with major changes in their agencies' security postures. As shown in Figure 2, the proportion of government employees working from home shifted from 11 percent to 65 percent in October 2020; this represents an increase of 491 percent.

Figure 2
Users Working From Home Before and During the Pandemic



Source: Osterman Research, Inc.

The proportion of employees working from home in October 2020 compared to before the pandemic has increased roughly six-fold.

SECURITY CONCERNS HAVE SKYROCKETED

Survey respondents were asked about the extent to which various security issues have become a concern since the pandemic began. As shown in Figure 3, 61 percent reported that not having the right solutions in place to secure their data and other assets has become a "major" or "huge" concern for them since the pandemic started. Nearly as many report this same level of concern about employees working from home insecurely, and nearly one-half report this level of concern about increased activity from cybercriminals and other bad actors.

Figure 3
Key Security Concerns Since the Pandemic Started
% Responding a "Major" or "Huge" Concern

Source: Osterman Research, Inc.

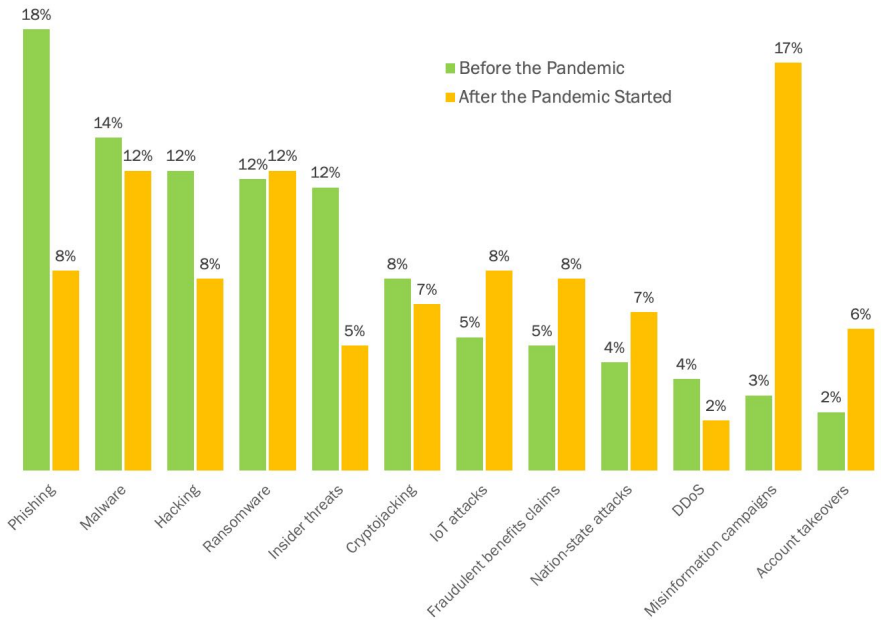
The concerns expressed by government decision makers are well-founded.

The concerns expressed by government decision makers are well-founded. Many government agencies, already cash-strapped by limited budgets, are now having to equip employees working at home with additional technology solutions and training to ensure that they can work as securely as possible. And, they have to allow government employees to conduct business and access sensitive data on the home networks that also support highly insecure connections to consumer home security systems, gaming devices, baby monitors, thermostats, and a raft of other devices people connect in their homes. Many of these devices are developed by contract teams, typically in East Asia, and cannot be upgraded to provide better security, as the teams that developed them no longer exist.

MISINFORMATION IS THE BIGGEST CONCERN

We asked government decision makers about what their single, biggest security concerns were before the pandemic started and now that it's underway. As shown in Figure 4, the four biggest concerns prior to the pandemic were phishing, malware, hacking and ransomware. While these threats have by no means gone away, concerns about misinformation campaigns have now become the leading concern, increasing nearly six times compared to their pre-pandemic level.

Figure 4
Most Serious Threats Before and During the Pandemic



Source: Osterman Research, Inc.

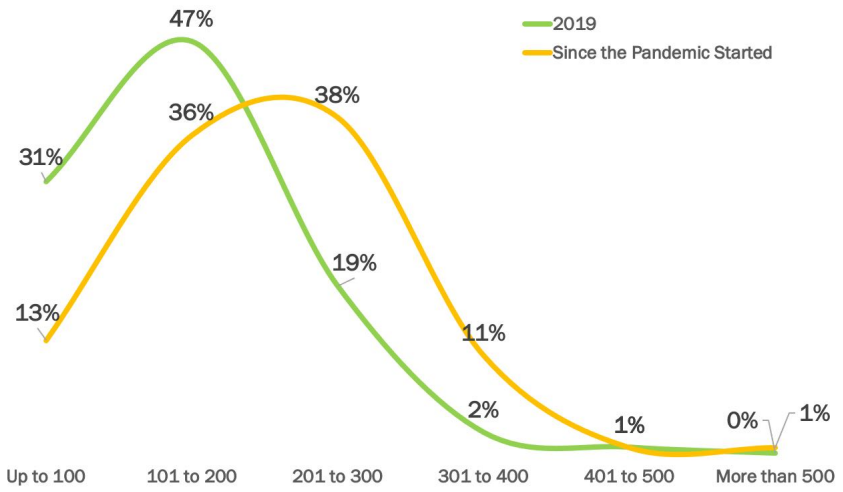
Misinformation campaigns have become the primary concern – especially in a presidential election year.

The fact that concern over misinformation campaigns grew was not shocking, especially given that it is an election year. The extent to which concerns about phishing dropped did surprise us, as it is a primary vector used by adversaries to carry out malware, ransomware and other attacks. Many election misinformation campaigns include phishing email components, as did the recent one across Florida, where the FBI and Office of the Director of National Intelligence Identified Iran as the main culprit.

THREATS HAVE INCREASED SIGNIFICANTLY

As shown in Figure 5, the level of threats and attacks directed against US and state governments has increased dramatically since the pandemic began. For example, while just two percent of agencies were experiencing up to 400 threats/attacks during a typical month prior to the pandemic, that has increased to 11 percent post-pandemic. Similarly, where 19 percent of agencies were experiencing up to 300 threats/attacks each month during 2019, that figure has doubled during the pandemic.

Figure 5
Monthly Threats/Attacks Before and During the Pandemic



Source: Osterman Research, Inc.

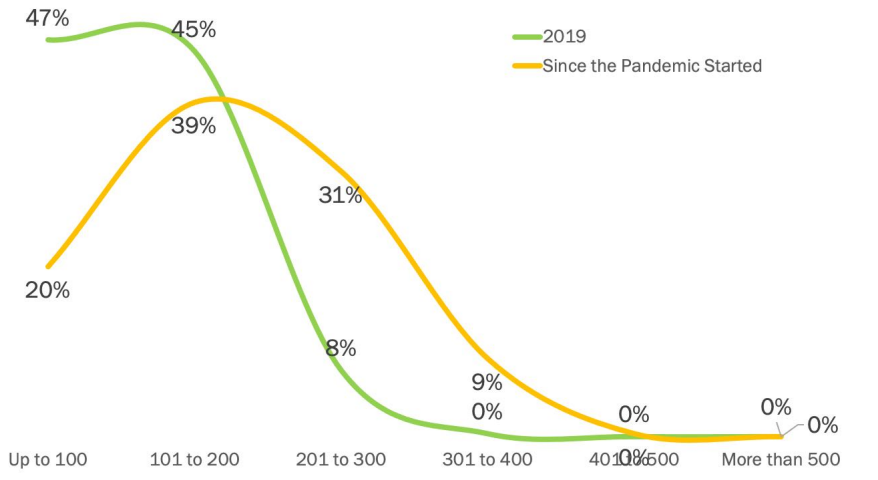
Although we asked the question in terms of ranges, by taking the mid-point of each range we were able to calculate the total number of threats/attacks that were received during a typical month in 2019 and since the pandemic started. We found that there was an average of 145 threats/attacks per month received by government agencies during 2019, but this number jumped to 203 attacks per month during the pandemic, an increase of 40 percent.

Prior to the pandemic, the average number of threats and attacks government agencies experienced per month was 145. Since March, the average jumped to 203. This is a 40% increase.

BREACHES HAVE ALSO JUMPED

Just like threats and attacks received during a typical month jumped significantly during the pandemic, breaches have also increased. As shown in Figure 6, fewer than one percent of agencies experienced up to 400 breaches during a typical month during 2019, but nine percent are experiencing this many now. Similarly, while eight percent of agencies were experiencing breaches during a typical month in 2019, that figure is nearly four times higher now, during the pandemic.

Figure 6
Monthly Breaches Before and During the Pandemic



Source: Osterman Research, Inc.

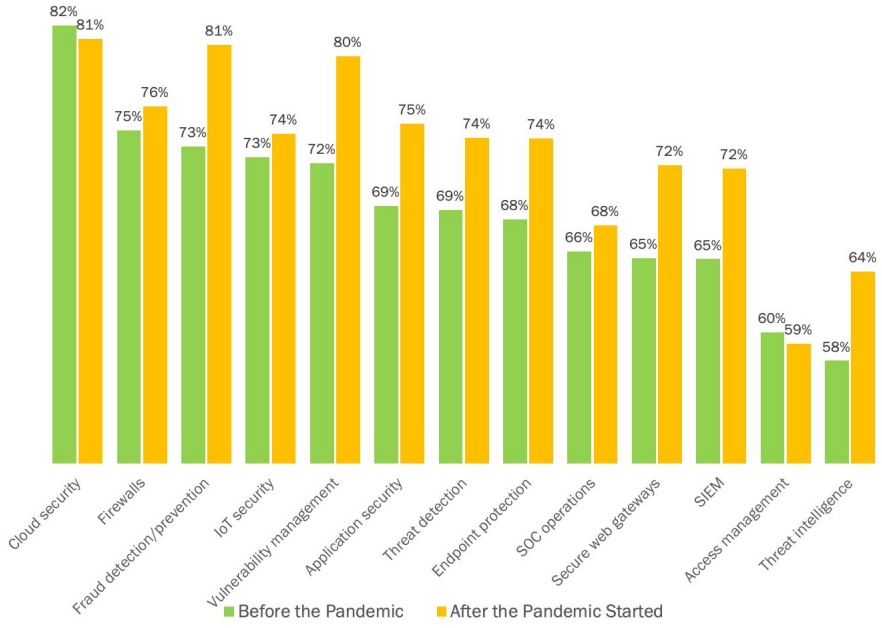
Using the same approach we took for calculating the total number of threats and attacks that agencies experience during a typical month, we found that the average number of breaches experienced during a typical month in 2019 was 112. During the pandemic, however, that average monthly figure has swelled to 181, representing an increase of 61 percent.

In 2019, prior to the pandemic, government agencies experienced an average of 112 breaches per month. Since the pandemic began, this number has risen to 180. This is a 61% increase.

SECURITY IS MORE IMPORTANT NOW

The survey asked decision makers to rate the importance of 13 different security technologies on a scale of 1 to 7, both before the pandemic and now that we are in the midst of it. As shown in Figure 7, the most important security technologies prior to the pandemic were cloud security, firewalls, fraud detection/prevention, IoT and vulnerability management. During the pandemic, the technologies that are considered most important have remained largely the same, but are mostly more important now than before the pandemic.

Figure 7
Importance of Various Solutions Before and During the Pandemic
% Responding "Very" or "Extremely" Important



Source: Osterman Research, Inc.

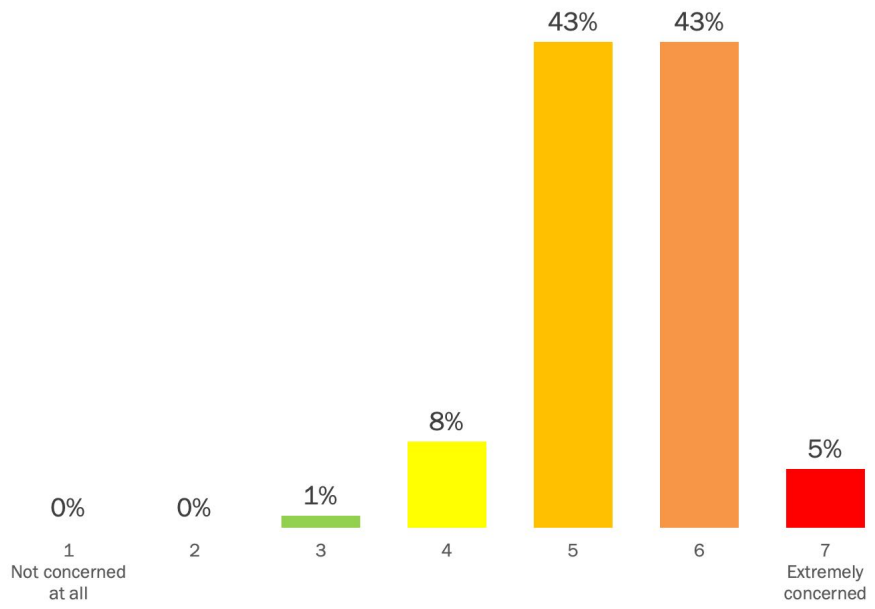
The technologies that are considered most important have remained largely the same, but are mostly more important now than before the pandemic.

Clearly, there were few significant changes in terms of what decision makers consider to be important from a technology perspective, but the importance they place on these technologies has changed since the pandemic started. As shown in Figure 7, only two technologies became less important since the pandemic started, and then only slightly less important. The other 11 technologies became more important, some significantly so, particularly threat intelligence, vulnerability management, SIEMs and secure web gateways.

DECISION MAKERS ARE CONCERNED

Decision makers are concerned about malicious cyber activities of various types that might disrupt state-level presidential election operations during 2020. As shown in Figure 8, 91 percent of decision makers are concerned about these types of disruptions, with nearly one-half "very" or "extremely" concerned.

Figure 8
Level of Concern About Malicious Cyber Activities That May Disrupt State-Level 2020 Presidential Election Operations



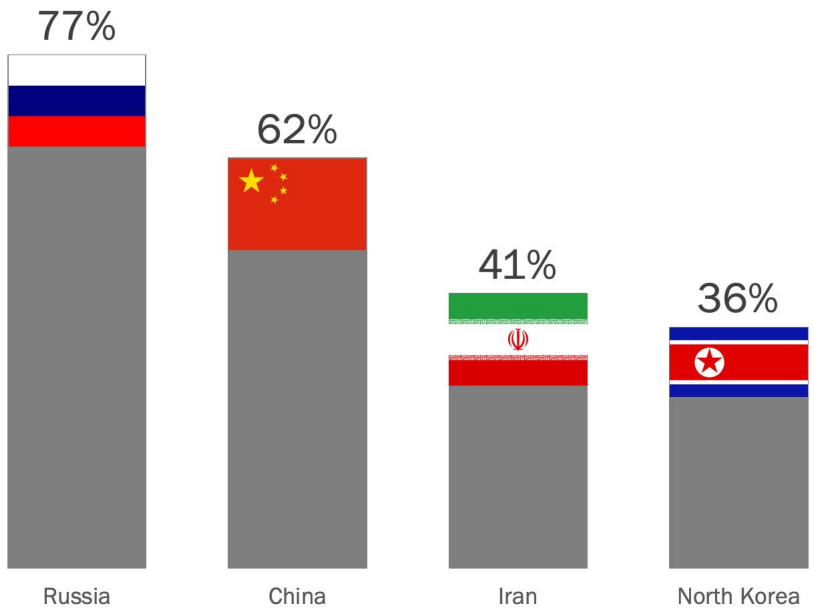
Source: Osterman Research, Inc.

Decision makers are concerned about malicious cyber activities that might disrupt presidential election operations during 2020.

RUSSIA AND CHINA…BUT WHAT ABOUT IRAN?

Not surprisingly, the focus of most government decision makers' angst about potential disruption to the 2020 US election process is Russia, cited by 77 percent of respondents as being "very" or "extremely" likely to disrupt things, as shown in Figure 9. Also, on the short list of potential disruptors in 2020 are China, cited by 62 percent of decision makers, Iran (41 percent), and North Korea (36 percent). Other potential threats to the US election process in 2020 that were cited in the survey are Egypt, Syria and Ukraine.

Figure 9
Likelihood of Various Nations' Attempt to Disrupt US Elections in 2020
% Responding "Very" or "Extremely" Likely



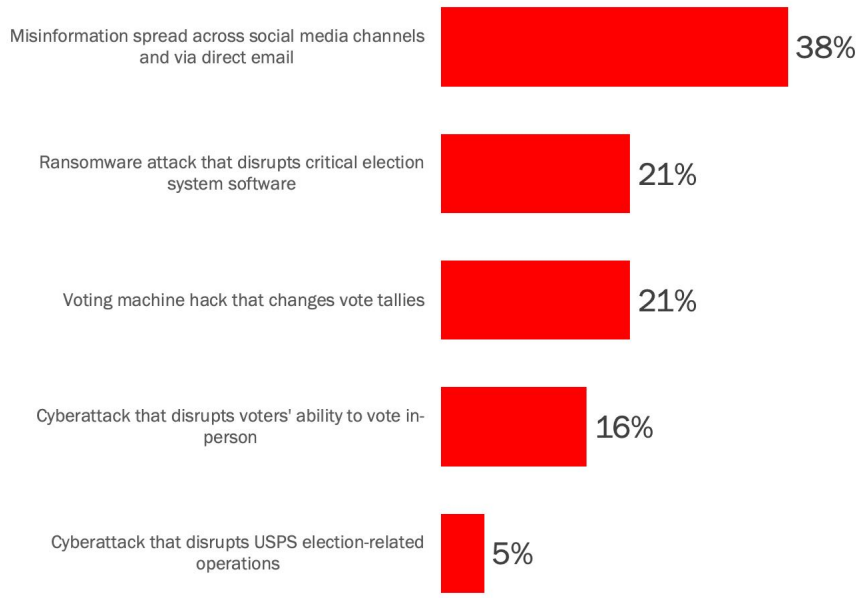
Source: Osterman Research, Inc.

The focus of most government decision makers' angst about potential disruption to the 2020 US election process is Russia.

MISINFORMATION IS ONE OF MANY THREATS

When government decision makers were asked what they considered to be the most likely mode of attack from nation-state actors who are known to back hostile cyberattacks against the United States, misinformation through social media and direct mail (phishing) were cited as the most likely threat by 38 percent of respondents. However, as shown in Figure 10, ransomware focused on election system software and voting machine hacks each were cited by 21 percent of respondents, while cyberattacks focused on disrupting personal voter activity were cited by one in six respondents. Only a small proportion of respondents believe that cyberattacks directed against the US Postal Service will be the most likely threat vector to be used by nation-state actors.

Figure 10
Most Likely Attacks by Nations That are Known to Back Cyberattacks Against the United States



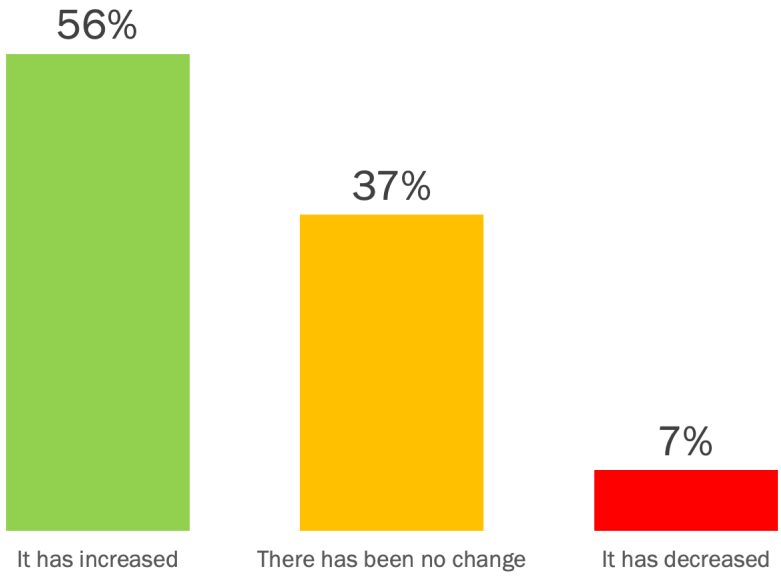
Source: Osterman Research, Inc.

Cyberattacks focused on disrupting personal voter activity were cited by one in six respondents [as the most likely attack vector].

MOST BUDGETS HAVE INCREASED

Despite obvious budget constraints faced by government at all levels during the pandemic, most agencies have increased their security budgets since the beginning of the pandemic, as shown in Figure 11. Another 37 percent of agencies have seen no change in their budgets, while only one in 14 have seen a budget decrease.

Figure 11
Changes in Government Security Budgets Since the Pandemic Began



Source: Osterman Research, Inc.

Government agencies, faced with the need to maintain services to the extent they can while also supporting a suddenly work-from-home workforce, have been forced to increase budgets to enable employees to remain productive. Many believe that IT and security decision makers should have been prepared for this eventuality in the context of deploying the right security technologies, continuity planning, maintaining the right resources available for employees, training their employees properly, and so forth. However, when budgets are tight, as they always seem to be in many government agencies, and security and IT decision makers are in their normal firefighting mode, it's not difficult to see why many agencies don't have the strategic foresight and financial bandwidth to deal with highly unusual events like the current pandemic.

Most agencies have increased their security budgets since the beginning of the pandemic.

Summary

The pandemic has been tough on US government agencies at both the federal and state levels. CISOs, IT directors and security directors report that threats, attacks and breaches are all up significantly during the pandemic compared to 2019. While they still fear traditional threats like phishing and ransomware, during the 2020 election cycle they now fear misinformation campaigns delivered through social media and email. On the plus side, security budgets have increased to help them deal with rising threat levels, but in the absence of the appropriate technologies to address these problems it may not be enough.

About Anomali

Anomali® delivers intelligence-driven cybersecurity solutions, these include Anomali ThreatStream®, Anomali Match™, and Anomali Lens™. Private enterprises and public organizations use Anomali to gain unlimited visibility, speed time to detection, and constantly improve security operations. Anomali customers include more than 1,500 global organizations, many of the Global 2000 and Fortune 500, and large government and defense organizations around the world. Founded in 2013, it is backed by leading venture firms including GV, Paladin Capital Group, Institutional Venture Partners, and General Catalyst. Learn more at www.anomali.com

ANOMALI®

www.anomali.com

@Anomali

news@anomali.com