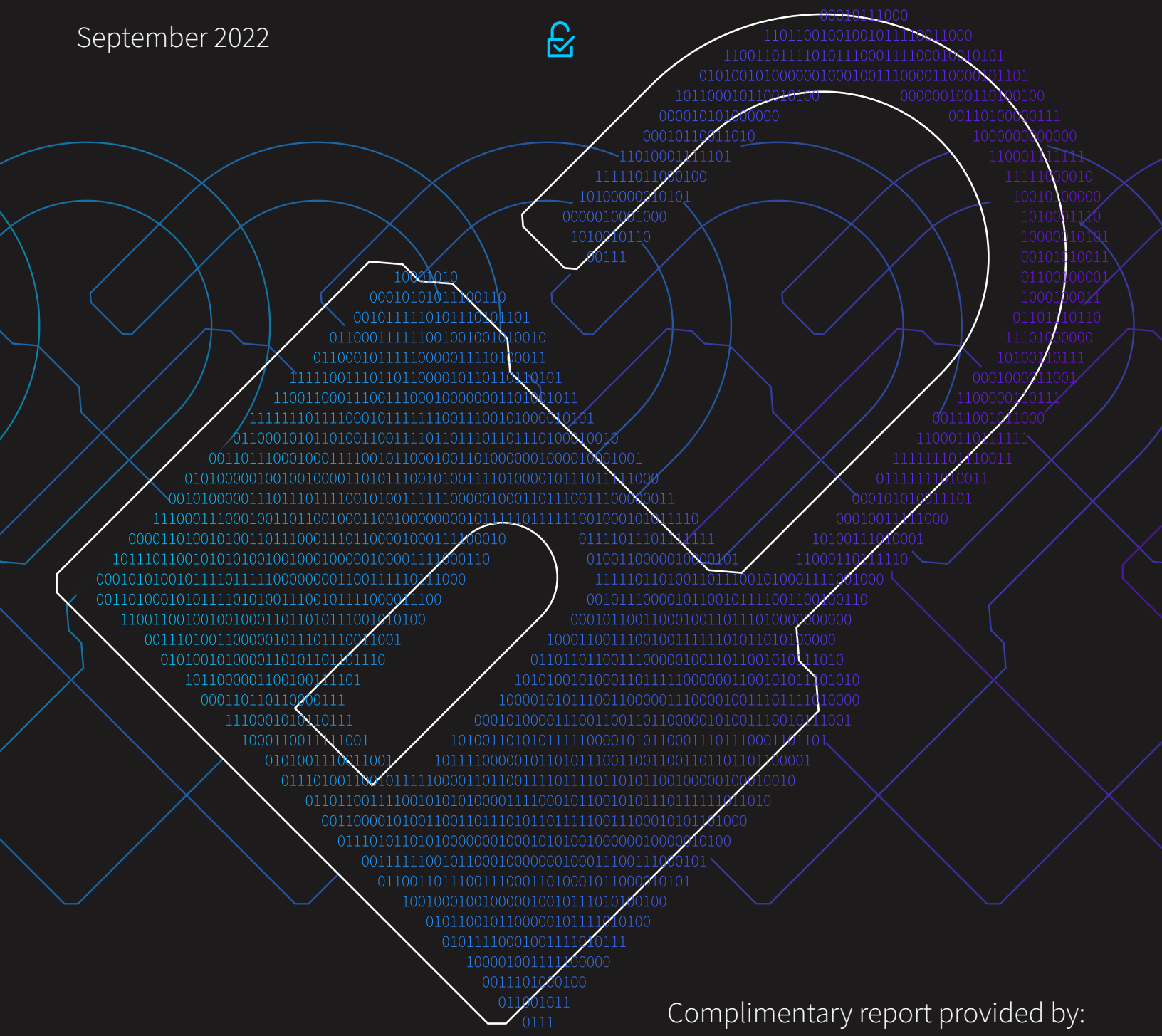
SECURITY NIST

AVANT 6-12 Report

September 2022



Complimentary report provided by:

CRYSTAL TECHNOLOGIES GROUP, INC. | AVANT

Introduction

Managing risk is getting harder every day. Bad actors have adopted their own internal enterprise organizational structure complete with HR, recruiting, training, finance, operations, and development teams. They use the same sales tools that the IT community knows and loves. They outsource, they broker their software, and they partner in their go-to-market strategies. Their market opportunity is extraordinary, and they have organized into a professional ecosystem that allows them to attack with impunity.

The vast majority (93%) of intentional breaches in 2021 were financially motivated with only 6% of reported incidents attributed to espionage[i]. However, meaningful breaches are not limited to threats external to the organization. Healthcare specifically has the highest rate of breaches where internal employees were the root cause of 39% of breaches, both intentional and unintentional[ii].

All organizations are targets
regardless of size, vertical, or profitability.

All organizations face some type of attack or breach from a wide variety of threat actors ranging from professional criminal syndicates that leverage the media and leaks to publicly attack their victims' reputations to increase their likelihood of ransom payout to state-sponsored espionage groups that are incredibly difficult to detect.

Copyright © 2022 AVANT Communications, Inc.

The dialogue around protection has shifted in three major ways.

1. First, organizations thought they could keep the bad guys out.
2. Then, the dialogue shifted from “What if it happens?” to “When will it happen?”
3. Now, organizations operate on the assumption that they have already been compromised and they simply do not yet know.

This final mindset shift is the fundamental principle that drives the concept of Zero Trust.

How do enterprises go about securing systems if those systems can’t be trusted? The security industry is complex and includes many different and sometimes opposed security frameworks that can be used. The framework that is increasingly winning within US markets is the Cyber Security Framework (CSF) published and maintained by the National Institute of Standards and Technology (NIST).

The NIST CSF is a widely accepted model for navigating security solutions. It provides a common language for organizations to communicate about cybersecurity risk and potential impacts. Just as important, the framework can be used for prioritizing cybersecurity investments so that money is spent on projects that will offer the highest impact.

This 6-12 report aims to discuss key trends impacting businesses’ cybersecurity. We will also introduce Trusted Advisors to the NIST framework and show how it relates to many different categories of security products and services. Trusted Advisors can leverage this knowledge to help enterprise decision makers get the most out of their technology investments while easing security pain points.

Copyright © 2022 AVANT Communications, Inc.

Security:
Ransomware Dominates the Landscape

What is cybersecurity? Cybersecurity is the art and science of maintaining trust and mitigating risk in our people, processes, and technologies to enable companies to go to market and win. Cybersecurity threats are coming from bad actors who are more well-funded and professionally managed than ever. That funding is increasingly coming from ransomware payouts.

Who are some of the bad actors companies are facing? State-sponsored groups have long been getting financial and logistical support from their governments, but in some cases, stolen assets are funding the group's activities — and more.

The Lazarus group is allegedly sponsored by the North Korean government and has actively targeted financial victims ranging from cryptocurrency exchanges to the US defense industrial base. In the latter case, the group could steal intellectual property that would allow North Korea to build advanced weapons and ballistic missiles and then finance their construction.

The Conti ransomware group openly aligned with Russia during the invasion of Ukraine and vowed to retaliate against Western companies if their governments intervened. Most recently, Conti — a professional criminal syndicate — initiated a ransomware campaign against the Government of Costa Rica and has publicly vowed to initiate and or support a coup attempt should the Government of Costa Rica refuse to pay.

Ransomware Outbreaks: Not a New Phenomenon

WannaCry is ransomware based on stolen code from the NSA that leveraged a vulnerability in Windows. A major outbreak spread in May 2017.

Petya and NotPetya are related pieces of malware that also leveraged the same vulnerability. While NotPetya disguised itself as ransomware, after infecting millions of computers in June 2017 it became apparent that its main intent was the destruction of data.

Copyright © 2022 AVANT Communications, Inc.

Threat Actors: Well-run Companies with PR and HR Operations

Criminal ransomware groups are also becoming more media savvy, using the threat of leaks to the press to leverage ransomware and extort payments from victim companies. Criminals know that news outlets are covering cybersecurity incidents closely, and that the threat of reputational damage can often result in company executives and their boards quickly authorizing ransom payments. If a company still does not pay, the ransomware group will then initiate a marketing drip campaign against their victim where they slowly release their victim's confidential intellectual property to the media.

> One of the more **interesting, mature things about Conti is that they often "go dark" or rebrand when they get too much pressure from the good guys.** That just goes to show how adaptive they are and really highlights their ability to play their cards with the media.

- AVANT's Senior Director of Security, Stephen Semmelroth.

Copyright © 2022 AVANT Communications, Inc.

Ironically enough, we know more about how ransomware gangs operate in a professional, business-oriented manner because of the Conti chat logs leaked by a security researcher. The Conti group has teams divided into different functions, with one team focused specifically on negotiations with victims, for instance, and another devoted to publishing information about victims on a web site. Conti's internal negotiators, who get a commission on collected ransoms, offer discounts for quick payment.

Tia Hopkins, Field CTO and Chief Cyber Risk Strategist for eSentire says

> **The bad guys are now organized. And they're doing the same things and using the same technologies** that we're using to scale our businesses, to have broader reach and to do things faster. Just as enterprises are leveraging partnerships, ransomware groups are partnering so that one that is good at initial point of entry will partner with a group that specializes in lateral movement and another that focuses on delivering payloads.

Think your company isn't big enough to be a target? Think again! The group bases ransoms on estimated revenues — information that they base on research from resources such as Dun & Bradstreet. Reports show several law firms and a building material supplier with revenues of around $20M annually among the victims. After they gain access, the more mature criminal ransomware groups will also hunt for internal legal contracts, insurance underwriting records, and financial reports and use that information to set an appropriate ransom amount. They only care about one thing: how can they make you pay!

Copyright © 2022 AVANT Communications, Inc.

Ransomware Driving Business and Political Push for Cybersecurity

The passage of the Cyber Incident Reporting for Critical Infrastructure Act in 2022 marked another milestone for businesses. The law requires "critical providers" — meaning utilities, hospitals, banks, transportation and energy providers among other industries — to alert the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours of a major cyberattack or 24 hours of a ransom payment.

Looking ahead, the Securities Exchange Commission (SEC) in March 2022 put forth a proposal that would require current reporting about material cybersecurity incidents.

> We are also **proposing to require periodic disclosures about a registrant's policies and procedures** to identify and manage cybersecurity risks, management's role in implementing cybersecurity policies and procedures, and the board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk. Additionally, the proposed rules would require registrants to provide updates about previously reported cybersecurity incidents in their periodic reports.
>
> - SEC

As "Europe's GDPR and California's CCPA led the way. Now the SEC is following in their footsteps with potentially punitive actions for a lack of accountability. We see other agencies following that lead as well. The takeaway here is that companies need to put in the work ahead of the regulatory push just as much as they need to be ahead of our adversaries," says Semmelroth.

Copyright © 2022 AVANT Communications, Inc.

Financial and Reputational Cost of Breaches

With additional regulation comes additional costs. Failure to report breaches in a timely fashion have several different costs and consequences, including fines and penalties by regulatory agencies, class action lawsuits, and more. Not only that, but a company's stock price, financial results and customer reputation have significant costs as well.

In terms of federal and state agencies, some recent data includes the following:

- February 2022: Equifax agreed to pay a minimum of $575 million for its 2017 breach in a 2019 settlement with the Federal Trade Commission. The settlement finally received formal court approval in 2022.

- June 2021: First American, a real estate settlement services company, agreed to pay a penalty of $487,616 to the SEC for violations against the disclosure requirements regarding cybersecurity risk and incidents

- August 2021: Pearson Plc, a publishing and education company, paid penalty of $1M to the SEC for violations. The data breach occurred in 2018.

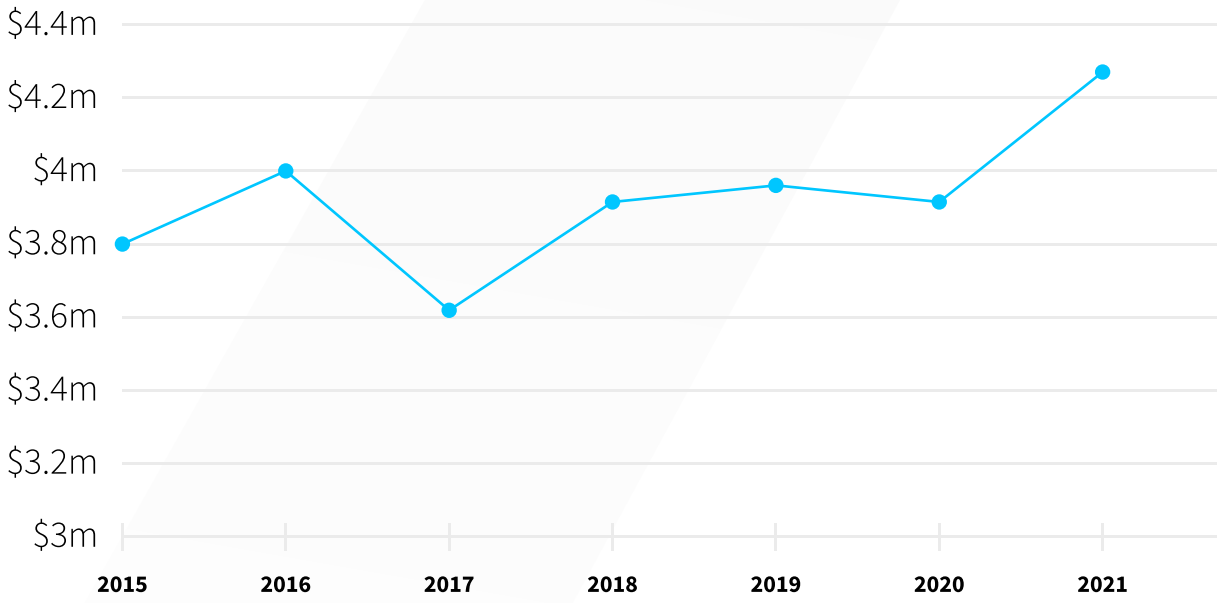
- May 2021: Minted, a U.S.-based marketplace, agreed to establish a $5 million settlement fund to settle a class-action suit filed for violations against the California Consumer Privacy Act (CCPA). Minted was the subject of an attack in 2020 that exposed data on over 4 million customers.

Copyright © 2022 AVANT Communications, Inc.

Direct Costs and Reputational Impacts

On a global basis, the average cost of a data breach increased by 10% in 2021, reaching $4.24 million, up from $3.86 million in 2020, according to the Cost of a Data Breach Report 2021 conducted by IBM and the Ponemon Institute. The US has continually ranked at the top of the list for costs: The average total cost in the U.S. increased from $8.64 million in 2020 to $9.05 million in 2021.

Average total cost of a data breach:



Source: Cost of a Data Breach Report 2021, IBM and the Ponemon Institute

Copyright © 2022 AVANT Communications, Inc.

Lost business costs account for 38% of total figures, including:

- The ability to book new orders or win new clients.
- Increased customer turnover.
- Lost revenue due to system downtime.
- Diminished reputation, which can increase the costs of customer acquisition.

In cases of ransomware, the ransom itself only accounts for about 15% of the total burden on the company.

Security Market by the Numbers

With the cost of breaches on the rise, it's no surprise spending on security technology is on the rise as well. Worldwide spending on information security and risk management technology and services is forecast to grow 12.4% to reach $150.4 billion in 2021, according to a forecast from Gartner. Security services including consulting, hardware support, implementation and outsourced services are 48% of spending at almost $72.5 billion worldwide.

Industry growth trends are powering engagements at AVANT, where data shows **Security Services sales grew 154% from April 2021 through March 2022.**

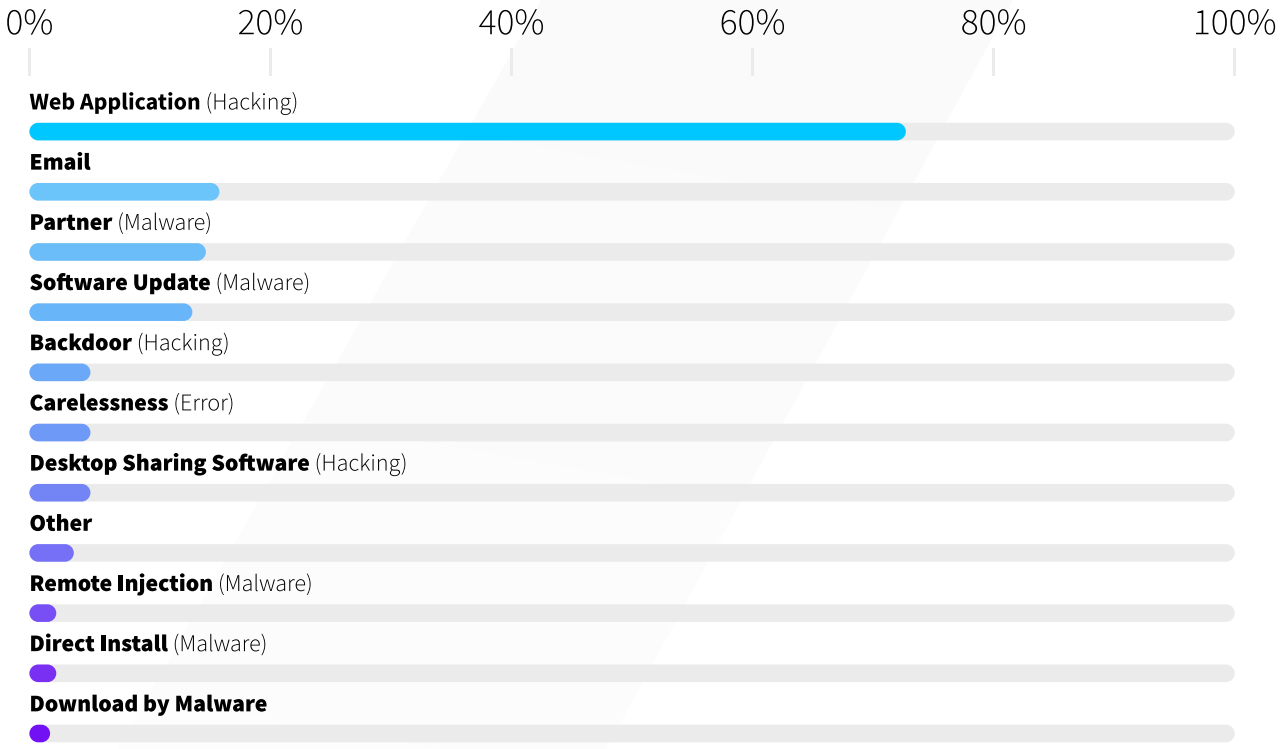
Source: AVANT's Trusted Advisor Growth Rate

Helping businesses target effective spending begins by understanding which industries are being targeted and how the threat actors that target those industries tend to operate.

Copyright © 2022 AVANT Communications, Inc.

Data Breach Reports

There are many private and public entities reporting on data breaches. Verizon's Data Breach Incident Report (DBIR) is one such long running and widely cited source of information. Some key takeaways from the 2022 DBIR report (which published figures on incidents in 2021): web application hacking was the top attack vector by incident count, followed by email. The report authors noted that it was the first time that partner and software updates were in the top attack vectors, in third and fourth place, respectively.



Source: 2022 DBIR Report

Top Action vectors in incidents (n=18, 419)

Top Patterns: System Intrusion, Social Engineering, and Basic Web Application Attacks represent 88% of breaches

Data Compromised: Personal (58%), Credentials (40%), Other (36%), Internal (14%) (breaches)

Copyright © 2022 AVANT Communications, Inc.

Targets by market vertical

Knowing patterns in specific market verticals is useful as well; although phishing and ransomware attacks are prevalent in every industry, there are some variations in the types of data that are targeted, for example. Manufacturing is one such example. In terms of attack frequency, DBIR tallied 585 incidents in 2020 and 270 incidents with confirmed data disclosure. In 2021, there were 2,337 incidents; 338 with had confirmed data disclosure, and money was the main motive (88%).

What Does the Data Look Like in Action in 2022?

According to Reuters, one of the tire manufacturer Bridgestone's subsidiaries was hit by ransomware in February 2022, forcing it to shut down production at its North and Middle American operations for nearly a week[iii].

Bridgestone is a major tire provider for Toyota cars. Just 11 days after Bridgestone's attack, another Toyota supplier, Denso Corp., was also hit by ransomware.

Toyota, which is already dealing with supply chain issues, may be a target for ransomware groups for reasons other than just money. Also in February 2022, Japan joined Western partners in restricting some Russian banks' access to the SWIFT international payment system and pledging $100 million in emergency aid to Ukraine. Within hours, Toyota supplier Kojima Industries Corp. said that it had apparently been hit by a cyber-attack, causing Toyota to shut down about a third of the company's global production.

Copyright © 2022 AVANT Communications, Inc.

DDoS and Cryptomining

According to AVANT's assessment data, collected from a wide variety of prospects working with AVANT-aligned Trusted Advisors, ransomware, DDoS attacks, intrusion, and email phishing attacks are the threats about which customers are most concerned[iv].

Distributed Denial of Service (DDoS) attacks are intended to compromise networks and systems availability. DDoS attacks, which include both network and application layer attacks, are a common type of attack that security providers have gotten good at defending. Cloudflare revealed that it mitigated a 17.2 million request per second (RPS) attack on a cryptocurrency launchpad and observed a botnet launching a 21.8 million RPS attack[v] . Attacks such as these have not been as prevalent — the DBIR reports that 1.3Gbps is the media size of DDoS attacks — but are often done in conjunction with other attacks as a sort of smokescreen.

Speaking of cryptocurrency, there is a different sort of stealing on the rise: resource theft in the form of cryptomining.

Backdoors and bitcoin miners are being actively delivered to susceptible Internet-facing servers via almost every vulnerability-of-the-week including the Log4Shell vulnerability which was publicly disclosed in December and now has had several patches available[vi].

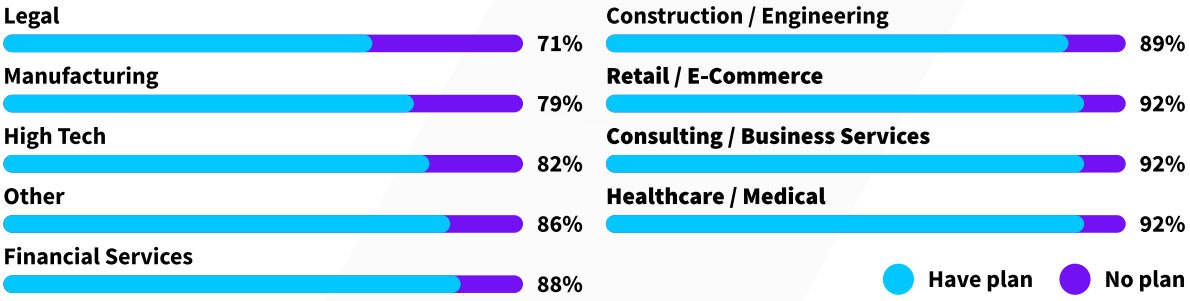
Sophos's cybersecurity researchers reported in March 2022 that cryptomining attackers began exploiting the Log4j/Log4Shell specifically in mid-January and are continuing to utilize that attack vector as a means of entry. Researchers expect the Log4Shell which is remote code execution (RCE)-type vulnerability in the Apache Log4J Java logging library is expected to persist for years given its widespread, almost ubiquitous, use and the constant patching priorities for developer teams.

Copyright © 2022 AVANT Communications, Inc.

The NIST Framework: The Corporate environment versus developer (CTO) environment

As noted in AVANT's 2021 State of Disruption report, the majority of companies in most verticals have plans for digital transformation, even in circumstances where they might not be fully deployed.

Industry vs Plans for Digital Transformation



Source: AVANT Analytics 2022

Given the state of security threats, how do businesses move forward with digital transformation efforts?

Highlighting that, Semmelroth again says, "Anytime you build something, whether you're building an app or a corporate IT environment, you need to start thinking about security from Day Zero," If you don't start with security, the cost to rework [and] go bolt on security later down the road, to go back and break out of your agile cycle to fix something that you could have done early in the process is about 10X of what it would have been in the beginning," he notes.

The NIST framework is a tool that can be used to guide investments in security to ensure that digital transformation projects grow the business, not just grow the attack surface.

Copyright © 2022 AVANT Communications, Inc.

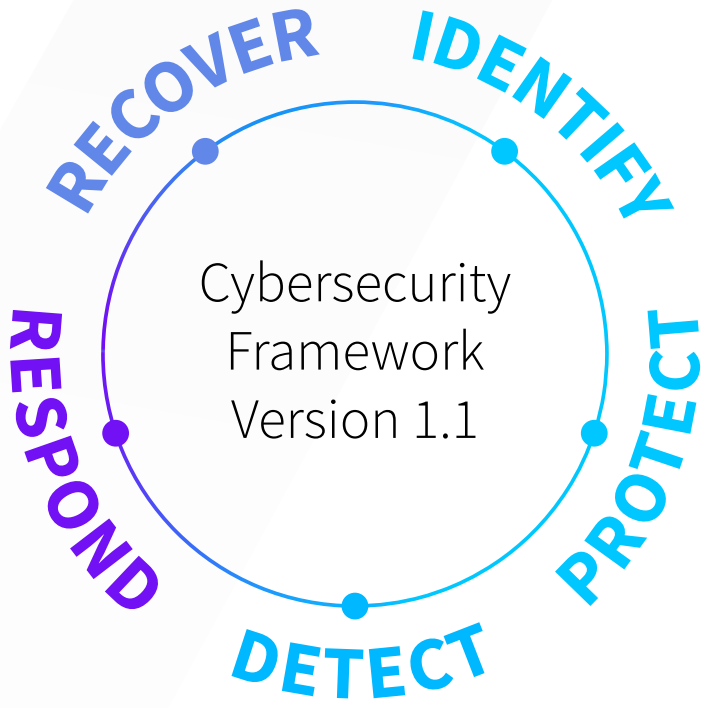
Explaining the NIST Framework and its Use in Enterprise Cybersecurity Programs

Having looked at the challenges and opportunities in the current cybersecurity landscape, let's look next at how the NIST framework fits into the picture.

As mentioned earlier, the framework that is increasingly winning within US markets is the Cyber Security Framework (CSF) published and maintained by the National Institute of Standards and Technology (NIST).

The NIST framework describes 5 core functions that are meant to be performed simultaneously and habitually to lower cybersecurity risks. Each function acts as a category for grouping actions companies can take to prevent, recognize, and mitigate threat actors.

The 5 core functions are:



Copyright © 2022 AVANT Communications, Inc.

Identify

Security teams cannot protect assets they don't know about. The main goal of the Identify function is to help organizations understand their environment and then prioritize their efforts in later stages. Mandated compliance standards and audits often create the baseline for these efforts. In the long run, the identification phase enables teams to be able to protect their stakeholders and their shareholders.

Activities in this function include:

- Asset Management – Continuous, long-term project, led by IT
- Business Environment – Short annual project, led by Security
- Governance, Risk Assessment – Short annual project, led by Security
- Risk Management Strategy – Short quarterly project, led by Security
- Supply Chain Risk Assessment – Medium project with smaller ongoing projects, led by Security

In essence, companies need to know what devices and services are a part of the internal IT landscape to secure them. It might sound self-apparent, but maintaining an accurate inventory is often an uphill battle given the constant, dynamic changes that allow companies to stay relevant in a competitive marketplace! Simply keeping a personnel roster while rapidly hiring and releasing employees is a challenge without the complexity that comes from mergers/acquisitions, equipment replacement, deploying new services in an agile environment.

To build out their Identify function, companies often turn to specialists in the field to evaluate their security posture. Those specialists, cyber security consultants, often conduct a myriad of both technical assessments and professional services discovery to truly understand the current risk posture. Cyber security consultants often assess the company's overall security program beginning with how the company earns its revenue and the security policies that enable them to go to market. Next, they conduct a technical assessment that can include employee interviews, technical scans, penetration tests, risk assessments, and gap analyses (often with the NIST CSF). While an organization may have goals for their security maturity, they may not have the talent or time to achieve those goals by themselves. One outcome of those assessments is often a prioritized, multi-year roadmap that helps the company "move the needle" in security and helps turn the overall vision into manageable projects.

Copyright © 2022 AVANT Communications, Inc.

Protect

The Protect function aims to deploy services that reduce risk to critical information and operations from threats. The proper protection will limit the amount of damage when cyberattacks do occur, to limit the blast-radius.

NIST lists the following as categories of activities:

- Identity Management and Access Control – Long term continuous project, led by IT
- Awareness and Training – Long term continuous project, led by Security
- Data Security – Long term continuous project, led by Security
- Information Protection Processes and Procedures – Long term continuous project, led by IT
- Maintenance (ex: patching) – Very large, challenging long term continuous project, led by IT
- Protective Technology – Small quarterly or annual projects

Traditionally, the Protect function stopped at a firewall. However, the concepts of Zero Trust and Defense in Depth changed the old way of thinking. Now, every asset, whether data or physical, logical, virtual infrastructure needs some sort of protection. Protection projects are usually cross-functional as they touch multiple company organizations. For example, shaping traffic on a network to isolate business functions and increase visibility requires both security and network personnel. Locking down user machines requires a joint effort between security and system administrators. Locking down the development pipeline requires a joint effort between security and developers. Building a Protect strategy that aligns with company profit targets is a challenge! The Protect function is often a combination of large projects with a variety of internal stakeholders and external service providers and products.

Copyright © 2022 AVANT Communications, Inc.

Detect

The next function is Detect, which encourages implementing practices that quickly recognize abuse by monitoring for system anomalies. Managed detection and response (MDR) and dark web monitoring are two examples of solutions designed for the Detect function. Activities in the Detect function include:

- Anomalies and events – Long term continuous project, led by Security
- Security Continuous Monitoring – Long term continuous project, led by Security
- Detection Processes – Long term continuous project, led by Security

The Detect function is traditionally led by Security and is where most organizations fail to hire, train, and retain talent internally that can monitor systems 24/7. One of the largest issues in the Detect phases is known as “alert fatigue” where Detection tools generate so many alerts that practitioners are drowned in a sea of false alarms. Often their response is to “tune” their sensors to the point that the sensors simply do not alert for anything. This happens often enough that IT business leaders question the efficacy of their own program and begin to explore outsourcing the Detect function.

Note: Many acronyms in the cyber security landscape like EDR, XDR, MDR, etc. often end in R for Response. However, in most of those services, the “response” is usually limited to either alerting or minimally blocking. The “response” in those acronyms is often more a marketing term than a full-fledged Response.

Copyright © 2022 AVANT Communications, Inc.

Respond

The Respond function includes all the actions teams take when they find a legitimate threat. This function is effectively the “break glass in case of emergency” phase.

Activities in this function include:

- Response Planning – Short term project, rehearsed quarterly, led by Security.
- Communications – Short term project, reviewed annually with Marketing, led by Security.
- Analysis – Short term project, led by Security.
- Mitigation – Short term, high intensity projects with many stakeholders, led by Security.
- Improvements – Short term projects as required, led by Security.

Here, corrective measures are used to mitigate the impact of an actual threat. Providers help prioritize the most important signals from the rest of the noise to ensure customers receive guidance when necessary and are not bothered for less important instances. One of the keys from the Response function is to triage whether an anomaly is a false positive, an event, an incident, or a breach.

Copyright © 2022 AVANT Communications, Inc.

- False positive – an anomaly that carries no risk to the business.
- Event – a small risk to the business that can be mitigated by the normal set of IT stakeholders.
- Incident – an all-hands-on-deck situation.
- Breach – an "Incident" that requires significant outside assistance and/or forensics.

One of the most important security measures companies can take is to purchase an Incident Response (IR) retainer from a trusted IR firm. Those retainers mean that companies are effectively pre-buying prioritized incident response consultants that can show up with no notice and help quarterback a complex response. IT leaders appreciate the buying process of an IR retainer because there are comparatively fewer technical requirements, fewer internal stakeholders to engage, and the contracting process is often simpler than almost any other service they need to acquire.

Recover

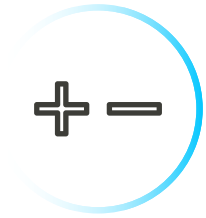
The Recover function focuses on quickly restoring data and normal operations following a security breach. It specifically focuses on response planning, improvements, and communications and typically includes having a team of experts ready to help after something goes wrong. Once a breach is remediated, the next step is to recover the data and focus on business continuity, which is a strategy to keep business operations uninterrupted at all times, despite disasters or failures. The Recover process is generally led by IT stakeholders and not security.

Copyright © 2022 AVANT Communications, Inc.

Mapping Solutions to NIST

What is the value of a framework? How do enterprises bring these ideas into practice? Organizations with mature security programs and the attendant resources (both budget and employees) can benefit even though they have built best practices and put tools into place for security.

Joe Martella, Senior Architect, IT security assurance for American Airlines, comments[viii] on the NIST framework: "The Cybersecurity Framework (CSF) five functions gives us better optics into where we succeed and fail in detecting/identifying risks, protecting our processes and data, and responding to and recovering from exposed vulnerabilities."



Reviewing the categories/subcategories with our product teams gives us the opportunity for retrospection into our own process to determine strengths and weaknesses.

The value of the NIST CSF, though, is that it can also help those organizations — often small and medium-sized enterprises — that don't have the same budgets or people in place.

The CSF offers a "ground level path for establishing a security program for businesses that have nothing or limited capability to implement a viable cybersecurity program. The very high-level nature of CSF categories and sub-categories essentially 'gets the ball rolling' focusing more on the 'what' rather than the deeper 'how' of a cybersecurity framework," Martella notes.

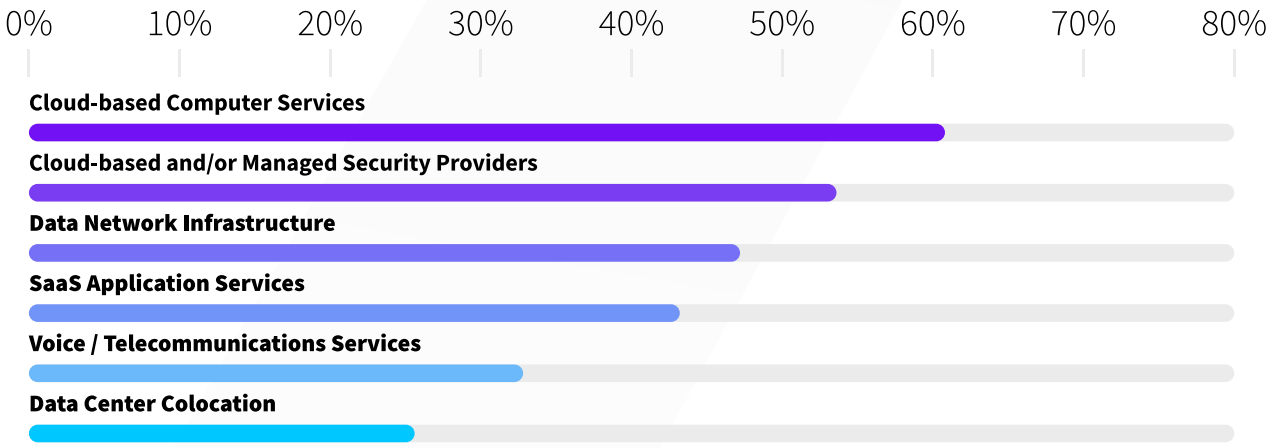
In the 2021 State of Disruption report, AVANT polled 500 U.S.-based enterprise decision makers at either the C-suite or Management/VP-level in IT, security, or finance. To qualify for the survey, respondents had to be involved in choosing or helping their organization to implement new compute infrastructure, network or voice technology including buying/ selecting new tools and services.

Copyright © 2022 AVANT Communications, Inc.

More than 40% of respondents believe that their internal teams are less than highly qualified to plan, manage, optimize, and troubleshoot the full range of their IT infrastructure, according to the report's findings.

Source: AVANT Analytics 2021

Companies in this condition are most likely to seek the services of a Trusted Advisor, in whole or in part, depending upon their specific circumstances. Trusted Advisors are already involved in many key discussions around cloud infrastructure, unified communications, contact center, SaaS, and network connectivity; some 67% of survey respondents said they engaged with Trusted Advisors for assistance with managed security services.



Source: AVANT Analytics 2022

Customers turn to Trusted Advisors for assistance with cloud services and selection criteria and consulting related to managed service providers (MSPs).

Copyright © 2022 AVANT Communications, Inc.

Relation of Zero Trust SASE to NIST Framework Components

One of the challenges for organizations is simply that it can be hard to make sense of the alphabet soup of frameworks, architectures, and marketing terms that prevail in the security industry.

For instance, many will have read about SASE, which AVANT has covered in a 6-12 report. SASE is a term that originated with Gartner which combines several network security functions (such as SWG, CASB, FWaaS, RBI, and ZTNA), with WAN capabilities (primarily SD-WAN). Like many such terms, the definitions change rapidly as vendors introduce new capabilities and converge existing features into formerly distinct product categories. Gartner itself has offered a separate category called "Security Service Edge" [ix] (SSE) which separates out the network-focused elements of SASE and includes SWG, CASB, and ZTNA as the necessary components of a complete security service edge offering.

Another very common term in the industry is Zero Trust, which is a set of principles that are used to organize and implement a security architecture, meaning it is a framework, too. The core of Zero Trust is that every resource, machine, code snippet, and user account could already be compromised and therefore are only granted access to limited resources and only when necessary and only after identities are verified. Put another way, zero trust is the overarching mentality that the NIST CSF implements. However, this is compounded by vendor marketing teams who jump on the Zero Trust bandwagon claiming they do zero trust when they only really do a small portion of the overall concept. A perfect example is Zero Trust Network Access (ZTNA) that only implements zero trust around how users access corporate resources but is still often misconstrued as Zero Trust.

Copyright © 2022 AVANT Communications, Inc.

Technologies and Solutions for the 5 NIST Cybersecurity Functions

The five NIST CSF functions provide a guide to evaluating security. Still, building a vendor selection strategy is challenging. The first step to choosing vendors for a security program is to acknowledge that there is no single silver bullet for protection.

Jim Campbell, Managing Partner with Opkalla, says

> Security is like Swiss cheese, right? There's no one product or service that's going to cover your clients' needs all together. **Every product, every service has a gap somewhere.** But how do you fill those gaps? You take a piece of Swiss cheese, add another layer and another layer and another, where **ultimately the end game is there are no gaps.**

Copyright © 2022 AVANT Communications, Inc.

Identify

While there are many different products used to help identify threats, organizing the tools and applying them in a coherent approach is hard for many companies. While an organization may have goals for their security maturity, they may not have the talent or time to execute them. During this stage, it is important to get a clear understanding of what data is important to a company's long-term business goals, the plan for achieving the security goals and cross-department investment in that roadmap.

One solution is security professional services often referred to as a virtual chief information security officer (vCISO). This is an outsourced CISO that helps a company build and maintain an information security program without hiring a full-time employee. This service can be especially helpful when aligning to compliance standards.

vCISOs can be incredibly beneficial for a company because of the shortage of qualified, IT talent and the expense that comes along with hiring them. Completing an inventory of the products a customer already has can be especially beneficial to figure out which ones aren't helping them achieve their security goals. The more complex the infrastructure or the more tools the client uses, the greater need to bring in someone that can help align a vision and reduce complexity.

The vCISO can provide an outside perspective on a client's internal infrastructure and provides added value through their extensive knowledge of the third-party landscape. The vCISO can then help enterprises develop a two-to-four-year integration plan as part of an overall security development program.

Copyright © 2022 AVANT Communications, Inc.

At some point, enterprises may decide to engage with cybersecurity companies for **professional services** — one-time engagements to evaluate a customer's security posture. Some examples include risk assessments, gap analyses, and **penetration tests**.

- Risk assessment is an examination of an organization's exposure to cyber risks and the determination of what needs to be done to reduce those risks. This involves analyzing the company's existing security program which begins at non-technical business outcomes before eventually analyzing technical measures. An organization's risk assessment should be updated regularly to keep up with evolving security threats and new security technology.

- Gap analysis is usually more specific in scope than a risk assessment and provides an overview of how assets are protected and what is not protected. A gap analysis can start with a security framework such as the NIST CSF to help identify which security controls need to be implemented.

- Penetration tests evaluate security controls and systems to find potential weaknesses at a given point in time. A penetration test emulates how a malicious actor will attempt to breach a company to determine how successful its security controls function in the real world.

Copyright © 2022 AVANT Communications, Inc.

When did you complete your last pen test or security assessment?

28% Other

24% < 6 months ago

21% < 12 months ago

16% 6 - 12 months ago

11% Never

Source: AVANT Analytics 2022

Which services are needed can depend on the maturity of the organization's security program and should be done regularly. Based on data from AVANT Analytics Research, 40% of companies surveyed by Trusted Advisors have done a pen test or security assesment within the last year. However, 21% have not done so in over a year, and another 11% said they have never conducted such assesments.

Using a third-party vendor can provide an external view of security risks that might have gone unnoticed due to infrequent reviews.

Copyright © 2022 AVANT Communications, Inc.

Protect

Once an overall program has been developed, some specific products in this category that can be implemented are:

- Multi-factor authentication
- Endpoint protection
- Firewalls
- DDoS mitigation

Although this is a category of security products that enterprises are very familiar with, as with other categories, a vCISO can be helpful in sorting through the huge vendor landscape to find products that have the capabilities a particular enterprise needs. This is especially true when moving from a hardware appliance-based approach to a cloud-based services approach — there is a fast-shifting universe of providers competing against the traditional hardware vendors in categories such as firewalls and DDoS mitigation.

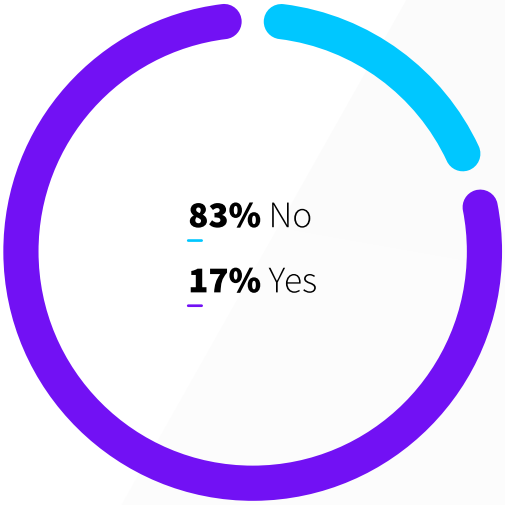
While there is a vast array of technologies that can be deployed for protection, employee training remains an important investment to make — employees are the first line of defense. An effective training program should include email security, password security, and even social media security to help employees stay safe online and protect their personal and company information.

Copyright © 2022 AVANT Communications, Inc.

Detect

Small and medium-sized enterprises should consider using managed services, which can address both the detect and protect functions. MSSPs can layer on proactive monitoring, patching, reactive troubleshooting, and administration. Based on data from AVANT Analytics Research, only 17% of companies surveyed by Trusted Advisors are using a third-party MSSP or SOC service. Of those who are, 54.6% have between 100 to 1000 employees.

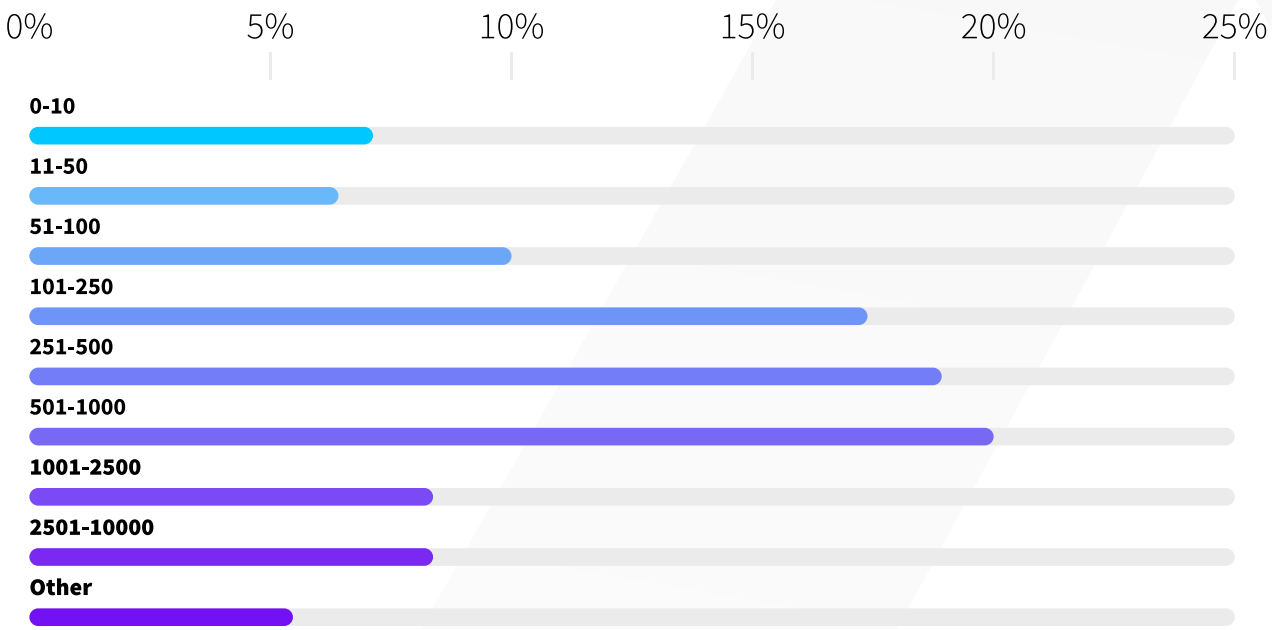
Percent of Respondents Using a Third Party MSSP or SOC



Source: AVANT Analytics 2022

Copyright © 2022 AVANT Communications, Inc.

% of Respondents Using a 3rd Party MSSP or SOC, by Company Size



Source: AVANT Analytics 2022

Products to consider for this function are:

- Endpoint Detection & Response (EDR)
- Managed Detection & Response (MDR)
- SIEM and Log Management
- Vulnerability scanning
- Behavior analytics

Another example of a solution for this function is threat hunting, which is a security practice that searches for indicators of compromise or concern within a network and on devices, no matter where they are located. Threat hunting has become especially important as more people work remotely.

Copyright © 2022 AVANT Communications, Inc.

Respond

Analysis and mitigation of an incident are critical to limiting damage. This can be one of the more time-consuming aspects of cybersecurity, meaning that if companies are already short-handed, outside resources need to be deployed. Having an incident response plan and provider in place before an attack is critical. Rehearsing that same incident response plan is often the key to mitigating a true breach when it does happen. One downside to highlight is when companies fail to engage an incident response retainer prior to a breach. In that case, their insurance company will dictate the response team and the client will have little to no ability to choose a vendor of their own accord.

Speaking of cyber insurance, companies may take comfort that their cyber insurance policies will cover the cost of forensic investigations and crisis management expenses, they should be aware that payouts can be denied due to failure to follow procedures or take prudent preventative measures. Researchers looking at the Conti group have also suggested that the group purposely targets companies with cyber insurance in place because they calculate that their chance of a payout is higher.

Recover

Businesses that need to restore data from backup or fail over to a disaster recovery environment quickly can implement Backup or Disaster Recovery as a Service (BaaS, DRaaS) to meet their needs. Another service that should be considered part of both the respond and recover functions is Incident Response and Forensics. This is an organized, scientific approach to investigate and remediate a security breach. It can be sold as an on-demand service or with a monthly retainer.

Copyright © 2022 AVANT Communications, Inc.

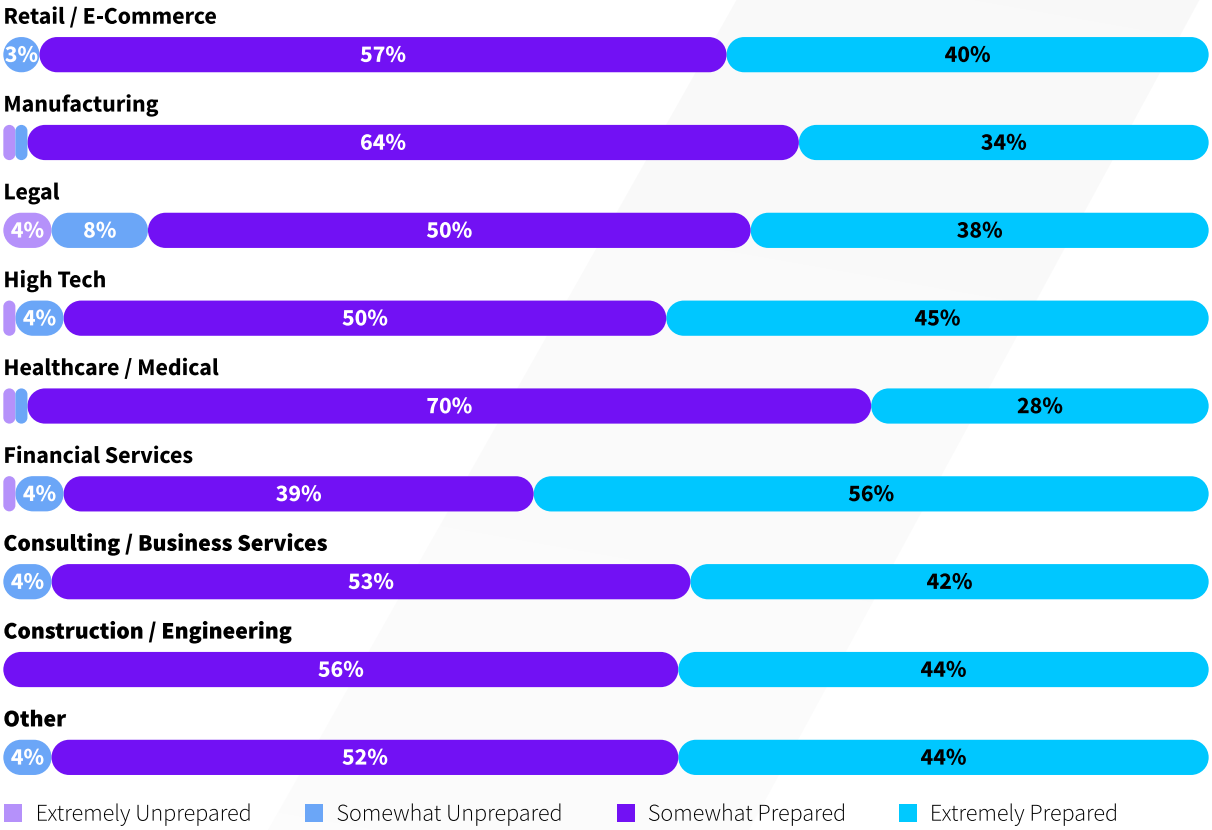
Moving from Reactive to Adaptive

So far, this report has talked about the NIST Cybersecurity Framework and the products and services that can be used in each of the five categories. If an organization has products and services in each category, do they have a mature cybersecurity program? Not necessarily.

Looking at data from the AVANT State of Disruption Report, one can see differences between different industries and different sizes of companies in their self-reported preparedness for cyberattacks. Survey respondents in the financial services market were the most confident, with 56% saying they are extremely prepared for attacks and only 4% are somewhat unprepared. There's still 39% of respondents who are "somewhat prepared," which means there is room for improvement. Interestingly, only 45% of respondents in high tech think they are extremely prepared, and 50% are somewhat prepared. Perhaps the best-educated consumers of technology are more aware than others that they remain vulnerable?

Copyright © 2022 AVANT Communications, Inc.

Preparedness for Cyberattack by Vertical



Source: AVANT Analytics 2022

This data shows that there is plenty of room for improving self-reported cybersecurity in almost every industry. While a framework like the CSF provides a roadmap, what is needed next is a maturity model to help with guideposts to show how far along an organization has moved.

However, self-reported readiness is not the metric that attackers use. While respondents in the healthcare sector reported that 70% feel they are somewhat prepared for an incident, the healthcare industry also has proven that they allow their own users too much freedom.

Copyright © 2022 AVANT Communications, Inc.

What is a cybersecurity maturity model?

NIST outlines four "Implementation Tiers" for the CSF, but NIST itself says the CSF isn't a maturity model. One maturity model, the Cybersecurity Capability Maturity Model (C2M2) comes from the US Department of Energy[x]:

> **A maturity model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline.** Model content typically exemplifies best practices and may incorporate standards or other codes of practice of the discipline.

according to the report authors.

A maturity model thus provides a benchmark against which an organization can evaluate the current level of capability of its practices, processes, and methods and set goals and priorities for improvement. A Trusted Advisor can play an instrumental role in helping measure progress in implementing the CSF and improving security systems within that framework. As is the case with security frameworks, there are a variety of security maturity models.

Maturity model: From Reactive to Adaptive

AVANT sees security deployed at three general levels, correlating not only to defensive tools, but also to the degree to which the organization establishes its own momentum around securing the enterprise and making sure key assets are safe.

As noted in the 2020 Avant 6-12 Security report "An Enterprise Decision-Maker's Guide to Maximizing IT Security," the three levels of security maturity are:

1. Reactive
2. Proactive
3. Adaptive

This framework was pioneered by our partners at Trustwave, a Chicago-based cybersecurity and managed security services provider.

Copyright © 2022 AVANT Communications, Inc.

Reactive is the use of traditional security products — antivirus, firewalls, IDS/IPS, email gateways, log collection, and the like — that are basic protection organizations need. The vast majority of SMBs are Reactive which is why many junior ransomware teams target SMBs.

Proactive security takes all the information and data fed to the organization by reactive technologies, and layers in security intelligence. Reports on cybersecurity issues and industry efforts and data sourced from cybersecurity experts focused on a particular vertical (threat intelligence feeds, for example) are ways to improve the value of existing systems and procedures. Automated alerting of high impact events is an example of proactive security. Most midmarket companies are somewhere between Reactive and Proactive. However, self-reported readiness is not the metric that attackers use. While healthcare reported 54% feel they are extremely prepared for an incident, the healthcare industry also has proven that they allow their own users too much freedom. The excess freedom within the healthcare industry is a strong contributing factor to healthcare having the highest rate of insider threats (both malicious activity and user errors) of any industry at 39% according to Verizon's 2022 DBIR.

Adaptive security focuses on taking proactive security up a notch and delivering outcomes for an organization. Examples of adaptive security include threat hunting, in which the organization engages an expert who specializes in security issues around a particular industry. That person (or service provider) does a comprehensive search for any evidence that the client organization is suffering from any of these specific breaches or attacks. Another example is the use of end user and entity behavior analytics to identify abnormalities, such as an unusual number of requests to a non-public web server, or an individual trying to access applications that they don't have permission for. Many financial institutions and other high-value, high-margin companies have adaptive security because they are under constant attack from determined adversaries.

Copyright © 2022 AVANT Communications, Inc.

Key Action Items

- The new paradigm in security: assume the bad guys are in the system. Plan accordingly.
- When planning, remember that there is no one solution, no magic bullet for security. Securing the enterprise is as much art as science.
- Internal expertise is often not enough. With security challenges broadening in scope and kind every day,few organizations will have the resources to move to an advanced “adaptive” security posture.
- If you not involving third parties, you are already behind. Engage a Trusted Advisor to help you on your security journey.
- The NIST model provides a useful baseline to map security project priorities. Use it to create near term (one year), and three- to five-year roadmaps.
- The market landscape for security products and services is complicated and constantly changing. Leverage the knowledge and relationships of a Trusted Advisor to help with validation and selection of security solutions.
- Baselining against the NIST framework is an ongoing process. Build a cross-functional team representing security, networking, compliance, Finance, IT management, and your Trusted Advisor and plan on regular reviews of security measures.

Copyright © 2022 AVANT Communications, Inc.

Key Roles Glossary

CISO
The Chief Information Security Officer historically has held responsibility for monitoring and controlling IT systems; mitigated and defended against cyberattacks; and coordinated incident response activities. The role is seeing a transformational change as CISOs evolve from being a security specialist to being business enablers. The CISOs will shift their focus from preventative and detective security controls to business enablement and risk management. The CISO is enabling the wider security program with strategic business insights as well as management and planning. Leadership of the security strategy and vision for the information security program is another key responsibility. In some industries, the dynamic is changing and CIOs sometimes now report to the CISO.

CISOs are tasked with the development and implementation of risk management processes to meet or exceed the governance requirements mandated by the board of directors and senior management, while ensuring the confidentiality, integrity, and availability of the organization's critical data assets.

CFO
A CFO is responsible for a company's financial operations on a day-to-day basis. Responsibilities typically include creating processes and setting controls for accounting functions.

CISOs work with CFOs to establish and attain the financial goals set by their organization's executive management. The CFO will work with the CISO to turn the organization's risk appetite and risk tolerance levels into a security program that maximizes protection of assets against potential threats while achieving budgetary goals.

CTO and CIO
A Chief Technical Officer of an organization is responsible for overseeing technical aspects of a company's operations, such as engineering, information security, hardware maintenance, and more. The CTO is typically a high-ranking IT specialist or very senior developer with a background in computer science.

Where CTO responsibilities tend to be customer-facing (outward), CIO responsibilities are often inward-facing; they may consist of managing and administering the company's servers, networks, and applications for internal business operations.

Both the CTO and CIO should be conversant in the business side as well as the IT side of an organization, with an understanding of how IT enables the business. That means that digital transformation efforts that run through these offices will also impact security programs.

Copyright © 2022 AVANT Communications, Inc.

Product Vendors
These are the companies that develop the software, products and solutions intended to protect data and other assets. Customers will likely find some options to be more effective than others, and some will work together in the same environment better than others. When they don't interoperate very well, they might cancel out one another's benefits, or cause the systems to work more slowly, due to the different products struggling for dominance. Vendors often rely upon MSPs and MSSPs to bring their products to market, though some may also sell through their internal sales forces. From the customer standpoint, direct sales efforts are led by people with sales quotas. Thus, the product they're offering may or may not be the best fit for your circumstances.

Managed Service Providers (MSPs)
MSPs use vendor products to deliver a security solution. They are not the developers of the product, although sometimes they may combine different products into a unified offer including a home-grown service that differentiates them against their competition. MSPs can often optimize a given solution to your needs and be able to function in a mode very similar to consultants (see below). In most cases, the buyer will have set options available but will be unable to make detailed requirements on which vendors and solutions will be used. This limitation is typically balanced by enhanced simplicity. Managed security services can also be provided by carriers working in an MSP or MSSP model. In most cases, carrier-based offerings are made available in conjunction with other offered services.

Managed Security Service Providers (MSSPs)
These are managed service providers who specialize in IT security to a much higher degree than most MSPs. They also have invested substantial sums of money in security operation centers.

Trusted Advisor/Consultant/Agent/Reseller/
This segment of the industry typically does not have an internally developed product or technology. They instead are designed to function as independent entities that can help you sort through the available options based on the specifics needs, budgets, and legacy infrastructure of your company. Their role is to do the necessary legwork, understanding the differentiators among the various offerings as well as those of the vendors that provide them. Aside from helping with the pre-sales phase of the engagement, they can also play a key role in deployment, optimization, support, training, and other facets of technology.

Copyright © 2022 AVANT Communications, Inc.

Acknowledgements

This report is brought to you by AVANT Analytics, a division of AVANT, where our mission is to provide timely research and insights for today's new and emerging technology services, including live and on demand reports, podcasts, briefings and alerts with the goal of accelerating technology decision making. AVANT enables Trusted Advisors to be leaders in informing technology decision makers with the market research needed to make purchasing decisions about today's new and emerging technology services.

Contributors

Alex Danyluk	Managing Director
Niko O'Hara	AVANT ANALYTICS Senior Analyst of Security, Enterprise Networking
Stephen Semmelroth	AVANT ANALYTICS Senior Analyst of Security
Brent Wilford	AVANT ANALYTICS Senior Analyst of UCaaS & CCaaS
John Paulin	AVANT ANALYTICS Senior Analyst of UCaaS & CCaaS
Chris Brennan	AVANT ANALYTICS Senior Analyst of CCaaS
Chip Hoisington	AVANT ANALYTICS Senior Analyst of Wide Area Networking & Mobility
Juan Ochoa	AVANT ANALYTICS Senior Data Analyst and Researcher
Brooke Kennedy	AVANT ANALYTICS Analyst
Jesse Garing	AVANT ANALYTICS Producer
Elise Zhang	AVANT ANALYTICS Digital Producer
Amy Ridder	AVANT ANALYTICS Editor
Jace Inman	AVANT ANALYTICS Graphic Designer

Copyright © 2022 AVANT Communications, Inc.

Appendix of Key Terms

Cloud Access Security Broker (CASB) is software that allows businesses to safely use the cloud by monitoring user activity and enforcing security policies between users and cloud applications. It is a type of Identity and Access Management technique that is used to regulate who or what can view and use resources in a computing environment. Specific data loss prevention policies can enable the detection of sensitive data in the network and stop that data from being transferred.

Remote Browser Isolation (RBI) is a technology that enables the user to access websites or applications over a separate server that then sends an image of that web page to the user's computer without accessing the resource from the user's machine.

Secure Web Gateway (SWG) enforces policies, supports regulatory compliance, and blocks unwanted and harmful traffic from entering a company's network. This is accomplished through a combination of malicious website detection (URL filtering), application controls, malware blocking (malicious code detection), and intrusion detection and prevention.

With **Zero Trust Network Access (ZTNA)**, every resource is already compromised, and every individual is treated as a malicious intruder until proven otherwise. Users and machines are granted access to specific resources only when necessary and after identities are verified. ZTA also isolates on the targeted application as opposed to providing access to servers in general, thereby making it more difficult for intruders to move laterally through the network, as is typically the case when Virtual Private Networks (VPN) are in use.

Copyright © 2022 AVANT Communications, Inc.

References

i 2022 Verizon DBIR, p. 25

ii 2022 Verizon DBIR, p. 61

iii https://www.reuters.com/business/autos-transportation/japans-bridgestone-reports-ransomware-attack-us-subsidiary-2022-03-18/

iv Avant 2020 6-12 Security Report

v https://www.securityweek.com/cloudflare-customer-targeted-record-https-ddos-attack

vi Log4Shell exploited to infect VMware Horizon servers with backdoors, crypto miners | ZDNet

vii https://www.securityweek.com/cloudflare-customer-targeted-record-https-ddos-attack

viii https://www.regulations.gov/comment/NIST-2022-0001-0082

ix https://venturebeat.com/2022/02/18/security-service-edge-splits-off-from-sase-in-new-gartner-magic-quadrant/

x https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf

Copyright © 2022 AVANT Communications, Inc.

SECURITY NIST

AVANT 6-12 Report

Copyright © 2022 AVANT Communications

v.3