AVANT

SECURITY

6-12 Report

Complimentary Report Courtesy of

12T Group

Technology Consultants

MARCH 2020

Complimentary Report Courtesy of

12T Group

Technology Consultants

We are excited to provide you with a complimentary copy of the AVANT Research & Analytics 6-12 Report on Security. As your Trusted Advisor, we aim to empower you with the information and resources you need to support your company's digital transformation.

There has never been a faster pace of change in IT, and the pace is accelerating every year. This 6-12 Report arms you with the most relevant information and insights necessary to assist you in evaluating your security needs over the next six to twelve months.

We look forward to supporting your IT needs and business outcomes to help you differentiate and stay ahead of your competition in this fast-paced and ever-changing world.

TRUSTED ADVISOR™

POWERED BY AVANT

Introduction

AVANT Research & Analytics: The 6-12 Report

This “6-12 Report” is developed by AVANT Research & Analytics with the assistance of technical teams within AVANT Communications, and backed by a wealth of data secured by AVANT in our normal course of business, our own primary research of end customers plus other reputable industries sources.

Additional AVANT Reports

AVANT 6-12 Report: SD-WAN
AVANT State of Disruption Study
Cloud Channel Survey

Our Mission

Our reports focus on today’s most disruptive technologies, where the pace of change is rapid. These companies or technologies, which may have been relatively anonymous just a few years ago, have now emerged as highly viable solutions to resolve the business needs that led to their creation. They have, in effect, disrupted the IT landscape, which is well known for its accelerating pace of change and innovation.

The 6-12 Report is designed to provide enterprise technology leaders with a contemporary and relevant overview of the featured subject for the next six to 12 months. Each subject is selected based on its opportunity for adopting companies to realize competitive advantages within their particular industry, market space, or company size.

All currency values in this report are expressed in U.S. dollars.

AVANT enables Trusted Advisors (agents, MSPs, consultants and similar channel partners) to support their business customers with IT technology decisions, with a specialization in disruptive technologies and solutions. We accomplish this with our:

- **AVANT Technical Specialists** that study the ins and outs of the latest IT technologies
- **AVANT Assessment Data** collected during thousands of customer assessments and resulting customer decisions.
- **AVANT Primary Research** of both customers and trusted advisors, to inform our decision making process.
- **AVANT Pathfinder** an IT Decision Making tool and repository of AVANT's market intelligence, allowing for comparative searches and intelligent search to help. (GoAVANT.net/Pathfinder)
- **AVANT Analysts** to conduct research and analyze data for in-depth analysis.

AVANT's Platform for IT Decision Making has assisted Trusted Advisors and their customers with thousands of IT decisions annually for customers of all sizes, from SMB to Fortune 500, providing us a large experience base and data set to reflect upon. Our role in supporting real world IT decision making with Trusted Advisors and their customers with leading technologies and solutions places us in a unique position to see near real-time market trends.

Our data is collected through sales efforts in conjunction with the Trusted Advisor community, through assessment data collected at the outset of the sales discussion, and through various market research tools, including surveys, interviews, focus groups, and external reports.

Key Takeaways

- Ransomware, DDoS attacks, intrusion, and email phishing attacks are the threats about which customers are most concerned.

- Customers' primary issues with their current security posture focus primarily on their fears regarding emerging threats combined with staffing and resource limitations.

- As many as two million security jobs are unfilled due to the lack of qualified people. This phenomenon is increasing the need for Trusted Advisors.

- Preparedness for attacks varies somewhat by vertical market with the highest levels of risk perceived by respondents in the Business Services and Medical sectors.

- We have shifted from a world in which the IT security budget is to be minimized, in favor of an environment in which the very survival of the business depends upon embedding security into every facet of the infrastructure.

- With the growth of things like toolkits and ransomware-as-a-service, extremely unsophisticated attackers can now purchase targeted exploits, enabling them to do significant damage.

- Companies across the broad market are moving to third-party managed security service providers at an annual rate of 5 percent RDI.

IT Security: The Landscape

Anyone familiar enough with the world of Information Technology to pick up this report has read about the hacks and cybercrimes that seem to have become a natural part of today's IT landscape. In fact, if all you've done is read about these attacks without ever having had first-hand experience, you are a very lucky (and somewhat rare) person indeed.

The exploits can range from the garden variety of phishing attacks aimed at virtually anyone who might bite, to attacks made as a political statement, moves by organized crime syndicates, or even acts of international espionage.

The most common threat vectors include Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS) attacks (DoS attacks with high volumes of computers), ransomware, man-in-the-middle attacks, zero days, (which exploit newly-discovered vulnerabilities), and, of course your garden variety of phishing exploits, viruses, worms, and general malware.

Modern attackers don't even need to be highly experienced or skills given that a wide variety of exploits have been productized into various, easy-to-use tool kits. Some criminals will even launch attacks in exchange for a fee.

Meanwhile, the industry is suffering a pronounced skills shortage in which as many as two million jobs are unfilled due to the lack of qualified people. This phenomenon is increasing the use of third-party contractors who specialize in security, as opposed to in-house teams, which have become dramatically more expensive.

Arguably, the most sinister attack is the Advanced Persistent Threat (APT) in which the cybercriminal zeroes-in on a specific target and invests whatever time and resources may be necessary to penetrate their infrastructure. In such cases, there is a particular objective and a particular payoff involved. It's very different from the type of attack in which a reasonable number of obstacles will redirect the bad guy towards some less-prepared souls.

The attack may target your access management, your administration platform, your applications, your endpoints, your network, or anything else on your attack surface. It doesn't matter. You and your team are on the hook for defending all of it by using a variety of technologies, my monitoring, by auditing, and, most of all by being ready, willing and able to properly respond when bad things happen. This translates to the existence of policies, procedures, tactical teams, effective budgets, and overall controls.

Ransomware is another insidious attack in which criminals, often gaining access through phishing attacks, encrypt your data and then offer to sell you the key. There is open debate on whether those ransoms should be paid, as opposed to restoring the data from backup. We will explore that issue in greater depth below.

Key Takeaways (Cont.)

- Companies across the broad market are moving to third-party managed security service providers at an annual rate of 5 percent RDI.

- Compliance is not security, and security is not compliance.

- Although user education is paramount, phishers are getting so sophisticated that even a well-educated user can fall victim to a well-crafted spearphishing campaign.

> **“Fast cars can go faster if they have good brakes.”**

Next add the complexities of defending a defined perimeter in the case of your data center, as opposed to your assets in the cloud. Think defense-in-depth for the perimeter defense and Zero Trust for your cloud security. Zero Trust is based on the premise that all devices on your network are compromised. Both of these will be covered in greater detail below.

Your general checklist for defense should include risk assessments, incident response plans, DDoS mitigation, endpoint protection, Managed SIEM, and perimeter security. Disaster Recovery-as-a-Service (DRaaS) is also a critical back up step to support mitigation when a successful attack occurs. You'll need to set up your infrastructure with role-based access controls that define who gets access to what. Anything sensitive will need to be encrypted, of course.

Some people view IT security as an otherwise avoidable (assuming there were no bad guys) pit of time and money that deflects attention from other investments more directly help to build the bottom line. After all, the criminal element should not do this kind of thing.

Others take a more optimistic view that, by amping up their security, they can now entrust their IT infrastructure to do things that their competitors would find far too risky to try – assuming, of course that they were using more basic levels of security.

To paraphrase one expert: “Fast cars can go faster if they have good brakes.” This highly profound statement is very correct despite its obvious incorrectness. No, the brakes don't make the car go faster at all. But it sure is easier to hit the gas when you know a good pair of brakes can drop that speed in a hurry, in order to keep you safe.

IT security is like that, too.

This 6-12 Report will help enterprise decision makers to work more effectively with trusted advisors to get the most out of technology while keeping their data safe. At the end of the day, that's what it's all about.

About the Analyst

Ken Presti develops the strategic framework and manages the process of leveraging AVANT's internal data and external data to drive high-value market research designed to help consultants, agents, channel partners, and other members of the Trusted Advisor community more effectively help their business customers understand and evaluate Information Technologies.

Ken Presti comes to the table with a wealth of experience in market research, survey development, focus group moderation, interviewing, and content development for the technology industry. His primary area of expertise is focused on go-to-market and channel strategies spanning the industry sectors of networking, cloud, security, and telecom.

A former Research Director of IDC's Network Channels & Alliances service, he has served as a Trusted Advisor to several key networking vendors and service providers. He has also led his own market research and channel advisory firm, Presti Research & Consulting, and has worked with other prominent channel consultancies. Presti specializes in combining empirical data, his own experience with the perspectives of industry leaders in a way that fully illustrates technology trends, business model evolution, likely outcomes, and strategies for success.

Contact us at research@goavant.net.

Download your copy at **goavant.net/security-report**

Security by the Numbers

It will surprise no one to read that cybercrime has become big business worldwide. According to the 2019 Annual Cybercrime Report by Cybersecurity Ventures, sponsored by Herjavec Group, the world will lose in excess of $6 trillion annually from cybercrime by 2021, up from $3 trillion in 2015. Worse yet, there's no reliable indication that this growth rate will plateau, let alone decline, during this time period. Meanwhile, the worldwide spend on cybersecurity products and services continues to grow commensurate with the uptake in attacks. These numbers vary widely among research institutions.

Gartner, for example, estimates the current spend at approximately $124 billion, representing a growth rate of nearly nine percent from 2018.

IDC forecasts that number at a more conservative $103 billion, though its projected growth rate is somewhat more bullish than Gartner's.

$258.9 billion
estimated value of cybersecurity market in 2025.

Source: Allied Market Research

$116.5 billion
invested into global cybersecurity in 2018.

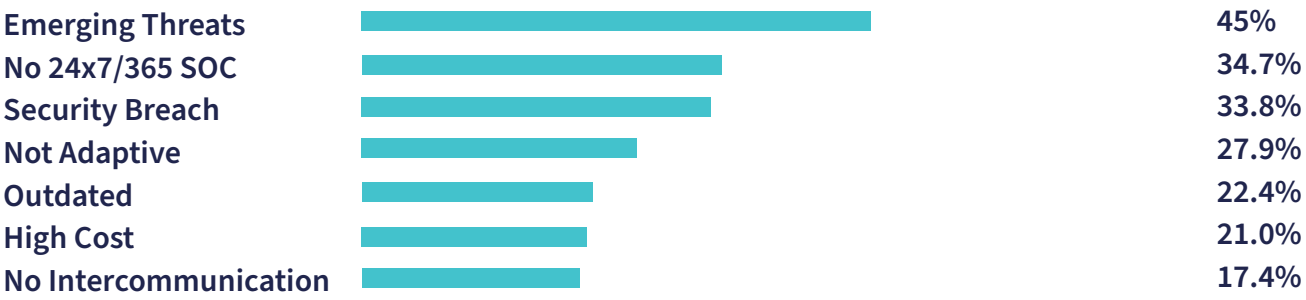
Source: Grand View Research

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. Their primary issues with their current security posture focus primarily on their fears regarding emerging threats combined with staffing and resource limitations plus a variety of other challenges, as shown in the table below.

Some enterprise customers have already suffered a security breach, feel the need for constant SOC support, or are looking for ways to maintain effective security at lower cost.

What are the prime issues with your current solution?

(By percentage of 414 respondents)



Source: AVANT Assesment Data

Current security solutions include a wide range of viable products and services on the market, ranging from endpoint protection as the most commonly deployed solution to software-defined perimeters at the bottom end of that deployment spectrum. Note that Intrusion Detection Systems (IDS) and Intrusion Protection Systems (IPS) both rank relatively high in this hierarchy, based on the types of threats most commonly faced by these companies. IDS and IPS typically go hand-in-hand in the selection cycle. The data also demonstrate strong links between IPS and DDoS mitigation, SIEM, and Log Management as most of these companies are looking to adopt strong, comprehensive security measures.

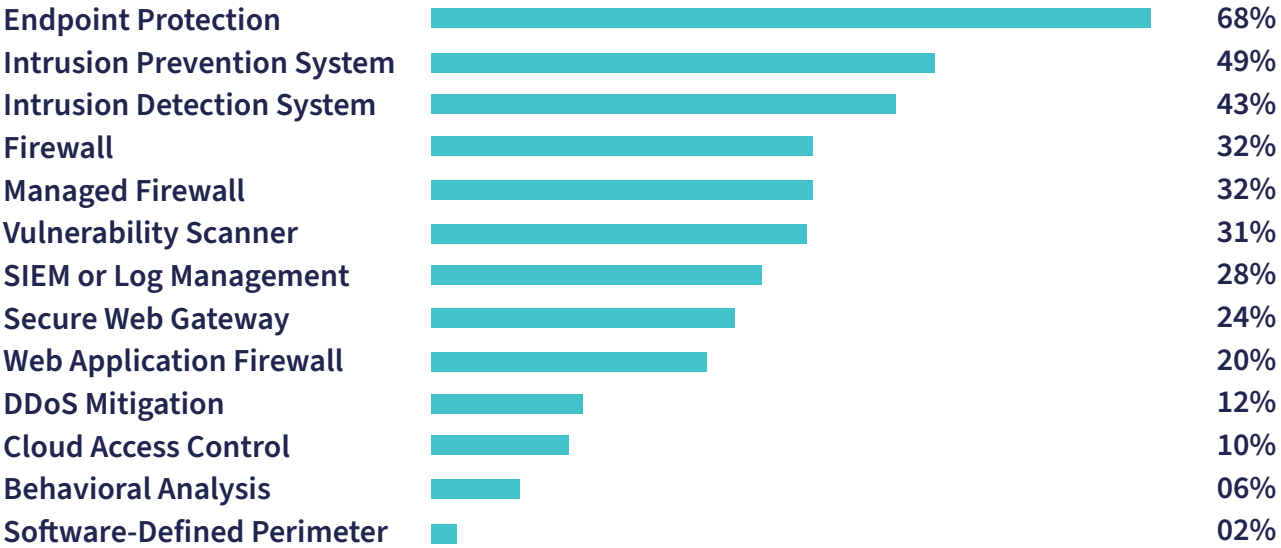
Companies looking to make changes with regard to firewall solutions are frequently looking to manage existing firewalls (61%) or move to a cloud-based solution (41%). Choosing "outdated" as the primary concern nearly doubles the likelihood that managed firewalls will either be implemented or updated.

Nearly three-fourths of the time when a firewall is added, IPS is part of the mix as well.

SIEM and Log Management are also on the upswing, given that security professionals are clearly recognizing the need for advanced security management and forensics tools. Desired SIEM features include Proactive Remediation (47%), and Alert & Notify (35%).

Which security products do you have in place today?

(By percentage of 653 respondents)



Source: AVANT Assesment Data

The Rate of Disruption Index (RDI)

AVANT Research and Analytics has conducted a study of the most disruptive technologies changing today's IT landscape, including SD-WAN, UCaaS, Hyperscale Platforms, Colocation, and Managed Security Services. Our goal was to assist our readers in assessing the rate of transition from one technology to a newer technology that is either taking its place or supplementing it. The "Rate of Disruption Index," or "RDI," represents the year-over-year shift in market uptake, as perceived by respondents to AVANT's State of Disruption Survey, conducted in the spring of 2019.

AVANT polled 300 US-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 the organization to implement new data network, voice, or compute infrastructure technology including buying/selecting new tools and services. Respondents include statistically significant subsets from the following five industries: Manufacturing Financial Services, Healthcare/Medical, E-commerce, and Consulting/Business Services.

As part of the survey, respondents were asked to compare their current progress within a technology transition with where that progress stood at the end of 2018. That data was then processed through a mathematical equation that quantifies that progress.

State of Disruption Report

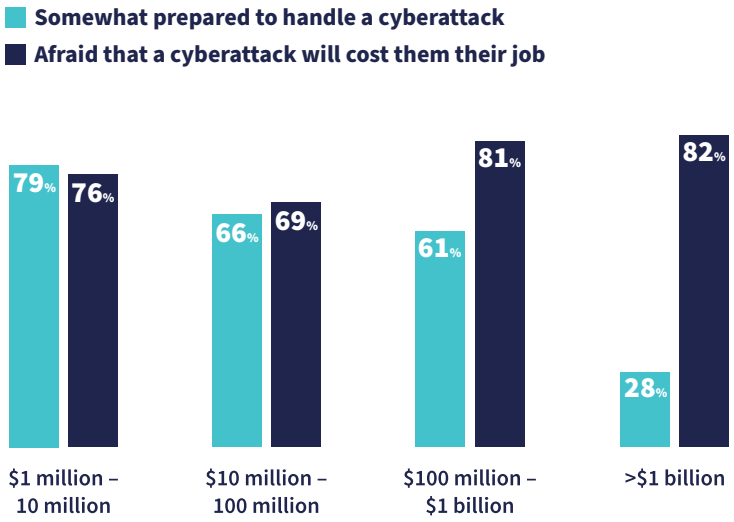
In the spring of 2019, AVANT launched an enterprise customer survey of 300 enterprise IT decision-makers who lead technology purchasing decisions. Respondents included statistically significant subsets from the Manufacturing, Financial Services, Medical, e-commerce, and Businesses Services verticals. Data taken from the survey were used to help support the development of AVANT's Rate of Disruption Index (RDI), which demonstrates the participants' perception of how quickly newer technologies are displacing older ones. For further details on the RDI, please review the accompanying sidebar.

According to the survey that serves as the foundation to the State of Disruption Report, more than half of the respondents are less than fully confident that their companies are prepared to handle a cyberattack today, and to mitigate whatever fallout might occur.

Respondents "Somewhat Prepared" or "Unprepared" for Cyberattack

Source: AVANT State of Disruption Report 2019

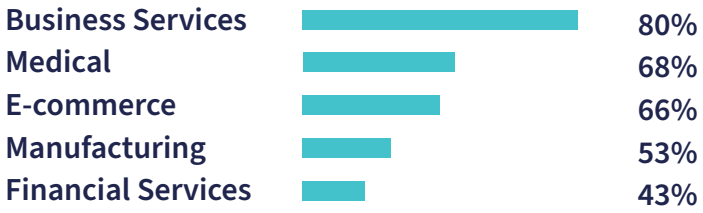
A substantial portion of companies with revenues less than $1 billion appear to be less prepared to handle cyberattacks than their larger counterparts. This is especially problematic, since the consequences of an attack are typically more pronounced in this segment. Small businesses often don't have the resources needed to recover from such a setback and go out of business as a result. Furthermore, as shown in the table below, a substantial percentage of respondents fear that a successful cyberattack against their companies will likely cost them their jobs.



Source: AVANT State of Disruption Report 2019

According to AVANT's research, preparedness for attacks varies somewhat by vertical market with the highest levels of risk perceived by respondents in the Business Services and Medical sectors.

"Somewhat Prepared" or "Unprepared" for Cyberattack



RDI (Cont.)

For example, respondents were asked to position, on a scale of 1 to 10, where their security infrastructure fell at the end of 2018, with "1" being 100% in-house resources, and "10" being 100% cloud based. We then asked respondents to again position and the same scale where their security infrastructure is expected to fall at the end of 2019.

In a scenario in which the average of all respondents was **"7"** on the first question, followed by an average of **"8"** on the second question, we measured the rate of disruption, accordingly:

(8-7)/7 = 0.1429

This computes to an RDI of approximately 14 percent, representing the rate at which business leaders expect to transition to a cloud-based model, and thereby displacing, or disrupting, the on-premises approach to security. To view this a different way, if the two models were tectonic plates pushing against each other, the RDI represents the earthquake, and its shift in plate tectonics.

RDI (Cont.)

This statistic will be used in this 6-12 Report, as well as in forthcoming 6-12 Reports on other technologies and business models.

The RDI is useful in understanding how adoption rates of new technologies are displacing legacy solutions as a comparative measurement to company sizes, market segments and as a comparative tool to other technology trends in a way financial market size does and growth does not, since the financial growth or revenue size of particular solution does not inform us, in and of itself, how much of an impact this growth is really having on a legacy alternative and normalizes this impact across different comparisons.

Interestingly, healthcare records are among the data categories most sought-after by cybercriminals due to the volume of personal information in those records that make them highly exploitable. Therefore, healthcare organizations face the most stringent industry requirements for breach notifications and cyber compliance, based largely on the HIPAA standard. This statistic in which 68 percent of medical respondents expressed concern about their ability to deal with a cyberattack is alarming, at best.

The State of Disruption Report also shows that overall respondents are moving to third-party managed security service providers at an annual rate of 5 percent RDI, which is one factor that is likely to help mitigate the talent shortage. When reviewed by vertical market, the e-commerce sector is moving in this direction more than twice as quickly as the broad market. At the opposite extreme, the Manufacturing sector scored zero on this scale. AVANT believes that many manufacturing companies mistakenly think they are at lower risk of attack and therefore don't pursue third-party solutions. However, their intellectual property can be of high value, particularly to bad-actor foreign governments. Manufacturers that maintain entirely in-house security face this risk.

RDI of Third-Party Security Services Adoption by Industry

E-commerce	Financial	Medical
12% RDI	**8%** RDI	**7%** RDI

Consulting	Manufacturing
3% RDI	**0%** RDI

Source: AVANT State of Disruption Report 2019

When reviewed by a mix of vertical market and company size, the leaderboard looks as follows:

1. **Retailers between $1 million and $10 million in revenue**
2. **Healthcare between $1 million and $10 million in revenue**
3. **Financial Services between $10 million and $100 million in revenue**

Similarly, companies among the broad market ranging in size from $100 million-$1 billion in revenue tend to be the most willing to adopt third-party security services, as shown below:

RDI of Third-Party Security Services Adoption by Revenue

$1-10m	$10-100m	$100m-1b	over $1b
1% RDI	**5%** RDI	**7%** RDI	**7%** RDI

Source: AVANT State of Disruption Report 2019

According to Markets & Markets, the global managed security services market size is expected to grow from USD 24.05 billion in 2018 to USD 47.65 billion by 2023, at a Compound Annual Growth Rate of 14.7% during the forecast period.

Escalating Threats

The data show that we have shifted away from a world in which IT security is partly an afterthought with a budget line item to be minimized as much as possible, in favor of an environment in which the very survival of the business depends upon embedding security into every facet of the infrastructure and every upgrade to that infrastructure. This observation is also matched by anecdotal accounts from people very deep in the IT security field.

“The attacks are getting more severe and they’re getting more common,” said Ray Watson, VP of technology at Masergy, a twenty-year pioneer in providing secure software-defined networking services for global enterprises. “Enterprises also facing attacks from many different directions. It’s no longer just the ‘hacker-in-a hoodie’ so to speak. It’s also unskilled ‘script kiddies’ [who use other people’s scripts and programs to launch attacks], competitive threats, insiders, cybergangs, all the way up to nation states.

“With the growth of things like toolkits and ransomware-as-a-service, an extremely unsophisticated attacker can now purchase targeted exploits, enabling them to do significant damage,” Watson added. “The rewards can be high, and the risks are low, especially in countries that don’t extradite to the United States. In short, it’s an unfair fight, and the advantage currently goes to the attackers. This is why successful companies partner with a managed security provider.”

Daily vulnerability scans leveraging AI and ML would not be overkill in this environment.

“More companies than you think have already been breached!” exclaimed Adam Burke, sales VP at Quest Technology Management, which conducts compromise assessments for customers, and finds active exploits roughly 70% of the time. “The attacks typically run in a six to 12-month cycle. In most cases they will spend that time looking for what they can steal and exploit while covering their tracks all the way. When they feel like they’ve got everything, they will withdraw, but will usually launch a ransomware attack on their way out.”

Ransomware is one of the most formidable types of attacks against corporations. In these exploits, the cybercriminals encrypt the company’s data, effectively holding it hostage until a ransom is paid. In most cases, the attack is enabled by a phishing campaign that fooled an insider into clicking on a malicious link. This threat vector has been under way for approximately 30 years, remains extremely effective, and continues to rise in frequency of occurrence.

> **“You don’t wake up one day and find that you have ransomware.”**

“In many cases it starts with a simple Microsoft Office file that has an embedded macro that then loads a web page that then loads a dropper, and then the dropper starts reaching out to command-and-control servers, and eventually starts infecting the LAN using an exploit like ‘Eternal Blue’ [which was allegedly stolen from the National Security Agency in 2017]. If you can capture it at any one of those first few steps, you can avoid a ton of damage. Unfortunately, most companies don’t start to catch it until after it starts to encrypt corporate resources and the ransom has been demanded. These days the ransom has a time on it, so it’ll say things like pay me two bitcoins now or pay me three bitcoins in four hours or five bitcoins in 24 hours. It puts a sense of urgency on the user to act quickly rather than take the time to make rational decisions.”

A few years ago, the conventional wisdom was to decline to pay the ransom and to restore the locked data from backups. These days, the cybercriminals can often reach those backups as well, rendering them useless. In addition, some data lockups can also be life threatening – particularly in the areas of healthcare and also municipal governments when 9-1-1 services are affected. If you do pay the ransom, there is no guarantee that the criminals won’t try to retain access to the network so they can repeat the exploit at a later date. Furthermore, news of the payoff will likely be posted to the Dark Web, which will attract other attackers who will now be aware of your willingness to pay.

“Companies need to discuss their response in advance based on circumstances,” added Masergy’s Ray Watson. “Many people will neglect to call law enforcement, thinking there’s nothing they can do. But sometimes the FBI can have the keys from other cases involving the same perpetrators, so it’s definitely worth a call.

In addition to phishing and ransomware, a wide variety of other threat vectors exist, including malware, man-in-the-middle attacks [intercepted data-in-motion], denial-of-service attacks, SQL injections, zero-day exploits and more.

According to the 2019 Verizon Data Breach Investigations Report (DBIR):

- **43%** **of breaches involved small business victims**
- **10%** **were breaches of the Financial industry**
- **15%** **were breaches involving Healthcare organizations**
- **16%** **were breaches of Public sector entities**
- **52%** **of the breaches featured hacking**
- **33%** **included social attacks**
- **28%** **involved malware**
- **21%** **were caused by errors**
- **15%** **were the result of insider misuse**

“These days we have far fewer introductory conversations in which we teach them why they’re vulnerable,” said Jack Danahy, senior vice president for security at AlertLogic, one of AVANT’s key partners in the IT security space. “They understand that security is an issue and that threats are all around them. On the other hand, the dynamic nature of the threats and the complexity around those threats can often lead customers to feel confused. So, we have to present with great clarity around what we’re going to do and how we are going to do it.”

Danahy further added that some companies have moved away from a viewpoint in which security is considered a defensive measure, as opposed to a strategic enabler through which they can more fully leverage their overall IT investment.

“The reason really excellent sports cars have really excellent brakes is so that they can go faster,” Danahy said. “What we’ve been seeing over the last few years is that forward thinking organizations have great plans for how to take advantage of the cloud or some new applications, but by automating or outsourcing security they actually begin to see security as an enabler of a new kind of business. In some cases, companies view security as insurance, but there are many things that companies want to do, such as pervasive things wired interconnectivity with their users and open relationships with partners that make this level of security important.”

By Danahy’s account, IT security enables companies to do more things with technology in a safer manner. Similarly, a car with good brakes is able to travel at higher speeds more safely by virtue of its increased ability to stop.

This newfound appreciation for the value of IT security clearly stimulates increased budget acceptance, yet plans for significant upgrades still require substantial consensus-building within enterprise organizations.

“Two or three years ago there was a significant increase in awareness of the potential for breach in both large and medium to small size organizations, and yet there was a failure to act in many cases,” said Lee Pallat, vice president of cloud and security strategy at Stratacore, an IT consulting broker based in Seattle. “There is certainly increased awareness and increased willingness to provide the budget for new security tools, and yet there can also be a fair amount of foot-dragging and delay. Even if you’re willing to spend the money it takes a fair amount of resources for a large or mid-sized company to put even managed security tools in place.”

While there is general agreement that budget and corporate willingness are moving in the correct direction, Ben Ferguson, a network and cloud architect at Shamrock Consulting, a Trusted Advisor in El Segundo, California, says this trend is often tied to company size.

“At the large enterprise we are seeing a lot more knowledge and understanding around how to create a security practice,” he said. “In the mid-sized and SMB segments, we see a ton of negligence. I’ve had a lot of C-level people tell me, “We don’t store social security numbers or credit cards in any of our databases, so we must be fine. And that’s pretty scary because that’s only a small segment of the attack surface.”

Ferguson says it’s a mistake to for Trusted Advisors to walk into their first meeting with a new prospect and ask them directly to identify their security vulnerabilities. “Nobody’s going to give those to you,” he said. “Plus, people don’t know what they don’t know. The important thing is to get a map of their network, their infrastructure, and their applications and then start looking to understand the Layer 1 through Layer 7 vulnerabilities. From the standpoint of the enterprise buyer, decision-makers should be willing to answer questions about how they respond to specific threats, and that’s going to open up the conversation to building and adjusting plans and identifying blind spots.

In this modern era, enterprise IT decision-makers must also keep in mind that protecting against the garden-variety of hacker is no longer sufficient. They must also be aware that governments, and those who represent governments, are also involved in efforts to steal data, product roadmaps, design features, and similar items of value.

The total cost of Enterprise Owner Security

- **Purchase, installation, monthly charges, and maintenance costs.**
- **The cost of remediating future breaches, (both financial costs and “soft” expenses, such as damage to reputation.)**
- **Cost of staffing or third-party management.**

“The widespread use of cybertools by nation-states is really changing the game,” said Leo Taddeo, the chief information security officer at Cyxtera, shortly before that company spun off its AppGate security line. “We have, of course, an increase in the sophistication of criminal groups, but what is really new in my view is the acceptance of cyber offensive tools by adversaries like China and Russia. It’s become normal for Russia and China to deploy these tools against our government networks and also our private sector. The risks have gotten worse and the threat has increased, so companies have been getting very sensitive to the potential for true harm to the enterprise.”

Leveraging his experience running a cyberinvestigative unit for the FBI, Taddeo recommends a risk-based approach, which means understanding your business, understanding what’s important to your business, and understanding how to get the most security value for your spending. “Many times, the adversary teaches us what’s important,” he said. “They understand what truly has value and how it can be monetized.”

Taddeo says company should adopt a layered defense, which includes a variety of measures aimed at extending the time it takes to penetrate while at the same time shortening the amount of time necessary for detection.

Your Security Posture: Is it Working?

Unless your company is truly starting from scratch with a greenfield installation, which is truly rare in the enterprise computing space, the first step in approaching your security posture will be a true and honest assessment of what is already in place. The operative term here is "true and honest." It may be tempting to gloss over newly discovered gaps or issues regarding the comprehensiveness of your company's IT security infrastructure. This is especially true if the discrepancies might reflect poorly on specific individuals. However, a problem found is nearly as crucial as a problem solved. Therefore, it is important to approach this exercise with as much honesty and integrity as possible in order to establish a broad base of protection that defends not only your most important assets, but also safeguards different routes among less important resources that can be used to gain deeper and more dangerous penetration. Trusted Advisors can plan an instrumental role in managing this process.

In a survey conducted earlier in 2019, AVANT Research & Analytics asked technology decision-makers to rank their cybersecurity posture on a scale of 1 to 10 with the rating of "one" representing no security posture; "four" representing reactive security; "seven" representing proactive security; and "10" representing adaptive security. Responses broke down as follows within specified company size bands by revenue. As shown in the table below, the cyber security posture steadily trended upwards as revenue numbers increased.

How would you rate your cybersecurity posture?

(Out of a value of 10)

Overall Average: 7.4

Source: AVANT Assesment Data

As your company evaluates its cyber security posture, place particular emphasis on the collection of supporting metrics, the identification of key areas in need of particular protection, areas in which necessary protection is not provided, and an assessment of specific risks, attack surfaces, and attack vectors. And, of course, the process culminates in a detailed look at how to mitigate any issues and execute improvements.

Organizations will often focus on protections for that single resource that they deem most critical or most valuable. They lose sight of the fact that the attackers merely need to access a vulnerable machine that has access to that critical resource, sometimes via multiple hops. Effective defense in this environment requires a detailed look at how systems are connected.

In most cases, this involves a thorough review of the infrastructure, including any cloud services used by the company. The enterprise customer's Trusted Advisor can play an instrumental role in ensuring the proper execution of this phase. A penetration test and a test of exploits against employees may be advisable. These services can cost between $10,000 and $25,000. Some companies may be willing to do them for free, but the fee-based alternatives are generally viewed as more comprehensive.

"I am a huge advocate of proactive threat hunting," said Trustwave's Steve Baer, vice president of sales engineers at Trustwave. "And by that, I mean a realistic threat assessment; not just a pen test not a port scan, and not something you've had done by the same firm for the last three years. I'm talking about a deep, under the covers, search for adversarial activity in your environment. I equate that to making sure your foundation is sound before you build a house on top of it. You might do an architectural redesign, but before you do any of that, make sure everything is sound."

Most of the customers participating in AVANT's assessment surveys were no strangers to third-party security assessments. More than 60 percent have had such an assessment conducted within the last year, nine percent have done so more than a year ago, and another nine percent have never done a third-party security assessment at all. The remainder were uncertain of whether such a test had ever been done at all.

It will be important to view security from the standpoint of defending your data center while at the same time providing the necessary protections to fully support your company's web-facing products and services. This will be explored in more detail below. For the time being, however, it is important to note that the company's local infrastructure will need endpoint security, a traditional firewall, or in certain circumstances a next generation firewall that incorporates a variety of otherwise disparate functions. Decision-makers should anticipate a need for a comprehensive solution that gathers log information from a wide array of sources and inputs, and then correlates that data with both known threats and behavioral analysis to uncover threats that might not have an existing signature associated with it. This function is typically built around the use of a SIEM platform that should be coupled with intrusion prevention and detection capabilities that can be extended to server-based or virtual machine-based devices.

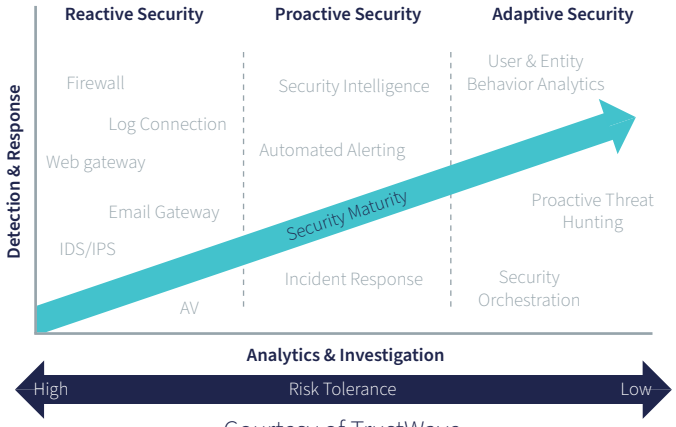
The alerts that arise from this kind of system need to be evaluated by qualified security analysts, and that's typically where an MSSP can be of service for companies that don't have the resources, or their own 24x7 SOC.

On the cloud side of the equation, most companies would be well advised to adopt a stateful firewall (which tracks network connections), a web application firewall, and DDoS protection, as well as making sure that the security features of the cloud service are properly configured from the customer point of view.

Three Approaches: Reactive, Proactive, and Adaptive Security

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

"Reactive" translates to the basic table stakes of engaging traditional security products with which IT professionals are typically at least generally familiar. These would include antivirus, firewalls, IDS/IPS, email gateways, log collection, etc., as shown on the chart below. These are typically the types of measures to be found in a middle-aged to mature organization that hasn't really pushed upwards into the higher forms of self-protection. All of these things are beneficial and positive, but they also represent a basic level of protection intended to react to cyber-incidents wither when they happen or shortly thereafter.



Courtesy of TrustWave

"Proactive" security extends the reactive level by taking all the information and data fed to the organization by reactive technologies, and then layering security intelligence on top of that value. This may include reports on cybersecurity issues and efforts within your industry sourced from cybersecurity experts focused on your particular vertical.

"In this scenario, the enterprise organization is really trying to understand what's happening specifically in your industry with the types of services that you would typically use," said Ron Hayman, AVANT's chief cloud officer and a Certified Information Systems Security Professional (CISSP). "So, if there are particular applications or hardware that is used in your industry then you're using that security threat intelligence to better understand what's happening in that space."

Hayman also pointed towards features such as automated alerting, which reduces fatigue in an IT operations center or a SOC, by limiting those alerts to messages of high importance. "So basically, this is about collating all that data into something that gives you a picture of where to focus your resources to protect the organization," he said.

“And then there is incident response, which is about investing in a plan and a team that can help you recover when a security incident happens,” he added. “This can be a team from your MSSP or from your own team and Trusted Advisor who are taking a step above monitoring and are trying to define how to better protect the organization.”

This initiative often includes Artificial Intelligence or Machine Learning, leveraging Big Data to help identify potential threats in key areas, and to determine what the response should look like in the event of an attack.

While falling short of actually fighting back, “Adaptive” security takes proactive security to the next level with a stronger focus on how to deliver the best possible outcome for the organization. Some of the things that fall into that category would be threat hunting, in which the organization engages an expert who specializes in security issues around your particular industry. That person does a comprehensive search for any evidence that the client organization is suffering from any of these specific breaches or attacks.

“This is about proactively using a tactical team to go look for what might impact your organization,” explained Hayman. “You can do that across your network, including the endpoints. Then there’s security orchestration, which is the automation of tasks that otherwise would need to be done by a security team or even an IT infrastructure team. Next, add behavioral analytics to allow you to understand what’s happening with your users and whether they are doing anything that is outside the typical thing that they would be doing on Friday at 2 am, for example. If it sees a behavior that it believes is out of the norm, it blocks or restricts access to it.”

In evaluating these positions, it’s important to understand the company’s relative maturity with respect to security, and the types of assets that most notably need to be secured. Oftentimes, compliance requirements actor into this equation, as well.

The cost of moving from one level to the next can be highly variable and dependent upon the number of users, number of locations, specific technologies, whether the capabilities are cloud-based or data center-based, as well as a number of other factors.

Most enterprises categorically fall into what we call the “proactive” phase of security; that is, they’ve implemented resources like intrusion detection, penetration testing, and a formal incident response plan. However, most have yet to achieve the “adaptive” phase of security, where their introducing proactive threat hunting, monitoring the dark web, and implementing end user/entity behavior analytics to identify abnormalities. Reaching this phase is pivotal to achieving security resiliency in a disruptive climate.

Coordinating Technology, Policy, Operations and Response

Although effective IT security decisions focus largely on the related technologies, a number of operational and managerial aspects must also be properly planned and executed in order to maximize the odds of success.

On the resource planning side of the equation, bear in mind that the industry is grappling with an ongoing shortfall of trained personnel. According to Cybersecurity Ventures, there will be 2 million more vacant positions in the cybersecurity sector than competent people available to fill them. That number is expected to increase to 3 million in 2021. The law of supply and demand dictates that this situation will drive up the costs of hiring and keeping those individuals, who are now enjoying brisk traffic in counteroffers from other potential employers. It's also fueling a substantial trend for outsourcing these responsibilities to MSSPs and Trusted Advisors who forge a specific business model and competencies in the security space.

According to Markets & Markets, the global managed security services market size is expected to grow from $24.05 billion in 2018 to $47.65 billion by 2023, at a Compound Annual Growth Rate of 14.7% during the forecast period.

AVANT's State of Disruption Report shows that companies across the broad market are moving to third-party managed security service providers at an annual rate of 5 percent RDI. This number ranges higher for specified verticals, especially E-commerce, which we measure at 12 percent RDI.

RDI of Third-Party Security Services Adoption by Industry

E-commerce	Financial	Medical	Business	Manufacturing
12% RDI	**8%** RDI	**7%** RDI	**3%** RDI	**0%** RDI

Source: AVANT State of Disruption Report 2019

Similarly, companies among the broad market ranging in size from $100 million-$1 billion in revenue tend to be the most willing to adopt third-party security services, as shown below:

RDI of Third Party Security Services Adoption by Revenue

$1-10m	$10-100m	$100m-1b	over $1b
1% RDI	**5%** RDI	**7%** RDI	**7%** RDI

Source: AVANT State of Disruption Report 2019

Whatever the means, security investments will always need to be balanced against the resource capacity and limitations of the enterprise organization.

"Typically, clients understand they have gaps they need to fill," observed Stratacore's Lee Pallat. "You have to guide them in a way that enables them to gradually fill those gaps with an array of managed services, of security tools that fit within the existing resource constraints of the organization. You also need to bring all the different stakeholders together and get them on board, and then push all of that through procurement at an executive level to make sure everyone is aligned."

In the midst of ensuring that planned technologies and available resources are properly balanced, it generally becomes more clear who the key stakeholders within the enterprise organization are likely to be. These individuals should be called upon to craft policies under which IT security should be managed. These policies need to define assets that are in the highest need of protection, who has authority for different aspects of enterprise security, operational requirements, and consequences for violations, In addition to security experts and IT people, Finance often plays a role, as does the C-suite management, Legal, and other teams.

One important consideration involves what types of data you want to collect, and how long that data should be preserved. The knee-jerk reaction for some people may be to collect as much as possible and keep it for as long as possible. But that can very quickly translate to a truly massive attack surface, to say nothing of the cost of securing it. Add on top of that the costs of any legal ramifications that can occur in the event of breach. All of these matters lead to very serious questions.

"What am I legally required to hold and for how long?" asked Trustwave's Steve Baer. "Question those things, because the longer you hold onto it, the longer you're responsible for it. And you're also responsible for the destruction of that data. Organizations need to be smarter about those things. If it gets extracted, your company is probably responsible for that, too."

AlertLogic's Jack Danahy said, "If I can be more rigorous in my examination of the data I'm going to store, how I'm going to store it, and how I'm going to link those areas of storage, it definitely reduces the complexity of my environment. And every time I decrease the complexity, I increase my ability to secure it. Taking the time to decide what to keep can be a real fact-finding exercise into what I'm going to look for, and the threats I'm worried about. A collateral benefit of performing that analysis is that I can become more targeted in how I'm going to use my security resources. I can develop a more proactive stance, based on the types of data I'm going to gather."

"It's a complicated issue and I think it's important to have a guide," summarized Hayman. "That's where the trusted advisor comes in to play. They have access to experts from the leading MSSPs. Ultimately, you want to partner with someone who can help you get all the way to your goal. That goal will sometimes need to change, and given the deficit in cybersecurity talent, the only way to do this successfully is to partner."

Trusted Advisors and MSSPs

Given the relative scarcity of skilled security experts, enterprise decision-makers will need to make careful choices about how their security postures will be managed and delivered. Perhaps there is someone in-house who can rise to the task, but that likelihood tends to be quite limited – especially when the risk is viewed in the light of security's constant changes. While a network can be built on existing technology to operate effectively well into the future, the same cannot be said of IT security, which is a sort of high-stakes "whack-a-mole" game in which attackers try to circumvent defenses, defenders try to fill those gaps, and attackers repeat the cycle by looking for new vulnerabilities.

In this environment, Trusted Advisors, often in conjunction with managed security service providers (MSSPs), will offer the best option – perhaps independently, or perhaps in tandem with one another. Depending on the security expertise within your organization, MSSPs might provide different functions.

"The smart CISOs [in enterprise organizations with substantial security expertise] are looking at the capabilities of their team and trying to figure out which low value tasks that can be outsourced to the MSSP, while the higher value stuff is done by the internal team," said Brian Stoner, VP of Channels & Alliances at ALTR, which offers data security-as-a-service. "That works down into the midmarket, but when you get into the SMB space, the MSSP typically becomes the outsourced security shop for a lot of them. That's a smart play for the SMBs because they really can't afford high-end security professionals. In their case, the MSSPs do the vetting and choose the products. The customers don't have to worry about the individual components."

In either case, Trusted Advisors clearly recognize the level of expertise involved in keeping their customers' data safe. They are therefore more willing to engage partnerships than ever before.

"Agents are typically aligned with MSSPs who focus on this issue all day long," said Gary Schick, National Partner Manager at Quest Technology Management. "Most agents and MSSPs will also have a quick reaction team, which will include people who specialize in this type of attack. These people might be their own employees, or they might include outside people whom they know and trust."

"We certainly support engaging with an expert partner in two aspects," said Lee Pallat of Stratacore. "One is having an incident response retainer which gives you access to a professional cybersecurity SWAT team to provide real-time guidance when breaches occur. The other aspect is for them to help you build an adequate response plan for when the breach occurs. What are your communication procedures, both internally and externally? What operational steps will you be taking to make sure you have all the necessary logging and tracking in place so you can identify what has happened and whether any data has been lost?"

Defense-in-Depth vs. Zero Trust: On-Premises vs. the Cloud

On the technical side, these response plans usually take on an expanded dimension, given that many companies are using both cloud services and customer premises equipment. Both of these environments share certain risks, as well as pose independent risks of their own. Focusing on either one at the expense of the other is almost guaranteed to make your company less secure.

In pure-play terms, the customer premises side is largely about securing a perimeter. You know the types of hardware being used and you know where those devices live. Your company is the sole arbiter of whether that infrastructure is properly secured and if it's not, it's usually not hard to identify the key suspects responsible for the oversight. For a long time, the mantra for securing the perimeter has been a concept called "defense-in-depth."

Defense in depth (also known as the Castle Approach) is an information assurance (IA) concept in which multiple layers of security controls are placed throughout an IT system. By bringing together a variety of security controls layered on top of one another in a collaborative rather than competitive way, enterprise companies can more easily detect and respond to threats by having more options for their detection and mitigation. Each one can address a different portion of the overall risk by improving database security, network access control, content management, perimeter management, compliance, endpoint and mobile security, intrusion detection and prevention, access management, and more. All of these can be applied across different layers of your infrastructure based on need and practicality, as shown below.

Don't forget that mobile devices, some of which may be owned and controlled by your employees and partners, can also cause significant risk. For those devices that do belong to your company, a comprehensive mobile device management (MDM) platform is likely in order. These systems can mitigate risk by properly accounting for inventory, scan for viruses, malware, and other issues, encrypt on-board data, provide general monitoring of the device, and even conduct a remote wipe if the device is lost or stolen.

Defense in depth (also known as the Castle Approach) is an information assurance (IA) concept in which multiple layers of security controls are placed throughout an IT system.

"Defense-in-depth really comes down to one thing, and that's visibility," said Trustwave's Steve Baer. "What's going on? What applications are in flight? What data is in use? Where does it go? Who touches it? And in some cases, there might be external partners getting involved. Does that introduce more or less risk to my environment? I need visibility into that supply chain."

A full complement of threat vectors must be covered in order for this strategy to work. For example:

- **Applications can be compromised through successful phishing attacks, faulty plug-ins, ineffective/underutilized patching policies, and other vulnerabilities.**
- **Data can be held captive through ransomware and related encryption.**
- **Endpoints may be penetrated by advanced persistent threats, spoofed credentials, viruses/malware, weak authentication followed by privilege escalation, or the occasional zero-day threat as it is released "into the wild."**
- **Networks may be improperly accessed through clients or servers.**
- **Sysadmin can fall victim through spoofed credentials or compromised equipment.**

"If defense-in-depth means that I need multiple kinds of protections to make my organization safe, I'm perfectly cool with that," commented AlertLogic's Jack Danahy. "But the problem is that people don't think enough about defense-in-breadth. Organizations will transform themselves digitally and head off into the cloud. And while they might have done a good job of securing the customer premises, when they move into the cloud, they haven't done all that thinking. They need to think broadly as well as deeply because we've seen organizations spend an overabundance of resources in a one area, and then be taken down by a simple failure in an area where they haven't spent as much time."

In some cases, they haven't spent any real time thinking about it at all.

"Many companies have moved data to the cloud without advising IT or InfoSec," said Masergy's Ray Watson. "So, they spin up an instance without knowing about securing buckets or default credentials or web application firewalls. Novices configuring these things can be especially problematic. Even under normal circumstances there are new and different attacks. There are new implications to think about, and the security posture can be quite different from what you're used to."

While on-premises infrastructure is largely about defending a defined perimeter, cloud computing is largely managed by the cloud service provider, such as Amazon, Azure, Google, Rackspace, or any number of other providers. The customer's visibility into how security is delivered is generally quite limited. That includes events, alerts, and activity logs. When selecting a cloud service provider, enterprise IT decision-makers should inquire about which activities are logged, and what level of forensic reporting they can access in the event of a breach.

In most cases, however, some aspects of security configuration can be determined by the customer organization. These would include patching/updating their software, effective management of how their network is connected to the cloud, and access control. Failure to properly execute that configuration can lead to a host of alerts or worse yet, gaps in security. This aspect requires a certain amount of caution as well. As most IT people will attest, an overabundance of alerts can bring about "alert fatigue"; a loss of focus, especially if most of those alerts are false positives.

["The cloud is not guilt-free computing..."]

"The cloud is not guilt-free computing," said Steve Baer of Trustwave. "The cloud is great, and faster, and usually less expensive, but it still requires the necessary due diligence and visibility. Don't ever get lured into the idea that because you're in the cloud, it's not your responsibility. It's still your data."

Much of the responsibility is defined by contract. Therefore, cloud customers are well-advised to carefully read their documentation in order to find out where the security lines are drawn. Most of the hyperscale security breaches have occurred because a business user of AWS or Azure did not properly configure a platform setting, leaving an exposure to be found later by a bad actor. Fortunately, there are Trusted Advisors who can help you find service providers that specialize in providing this type of assistance. Traditional hosting companies, such as Rackspace and Ntirety have become experts in managing AWS, Azure and GCP solutions, including cloud security management.

"Many enterprises are completely unaware of the managed hyperscale services available from MSPs" says Drew Lydecker, president and co-founder of AVANT. "It's become impossible for an individual to keep up with all the thousands of new features and changes hyperscale's are deploying each year. That's where MSPs excel. They stay on top of all the changes and help companies use platforms more effectively and securely."

Given that the perimeter-based approach of data center security is far too limited to meet the needs of cloud computing, the concept of "defense-in-depth" is rapidly giving way to a new, cloud-centric approach called "Zero Trust." One can make the case that Zero Trust works with the assumption that the entire network is already compromised. That is a bit of an overstatement, but Zero Trust is indeed based on a lack of trust in devices and machines.

"One part is knowing how to do authentication around users, around groups and around roles, explained Ray Watson of Masergy. "AI and machine learning can be used to watch for anomalous behaviors, triggering alerts very similar to what happens when there is a weird charge on your credit card."

Taking that one step further, the use of multifactor authentication is typically a good idea. In most cases, this involves a code being transmitted to the user's mobile phone via SMS. The user then enters that code into the application interface and, if the code is entered correctly, access is granted. While multifactor authentication is not an absolute guarantee that unauthorized people will not access your resources, it is an important layer of extra protection that is neither expensive nor especially difficult for individual users.

"Instead of thinking we are going to be able to defend all attacks, it's really coming down to reducing dwell time which is how long the bad guys are inside," Watson added. "It's also about segmentation, which is really about making sure that if someone does get in, they can't gain access to the corporate jewels, so to speak. Many people today are talking about managed detection and response, in which we see when an attacker penetrate and then immediately act to minimize the damage."

"It's become impossible for an individual to keep up with all the thousands of new features and changes hyperscale's are deploying each year."

Some experts make a valid case that Zero Trust and Defense-in-depth are often best used in conjunction with one another. This is especially true in hybrid environments where the cloud is used in conjunction with on-site IT infrastructure. In either case, both have their pros and cons, according to Brian Stoner VP Channels & Alliances at ALTR, a Trusted Advisor that specializes in data security as a service.

“With defense-in-depth, the additional layers [of complementary security products] give you greater opportunity to trip up the attacker,” he said. “The problem is that you’ve now got all these logs from various products and devices, and all that data can overload your SIEM [security information and event management] platform. On the other hand, Zero Trust makes a lot of assumptions that can be difficult to implement. The other challenge is how to handle third parties and BYOD without assuming undue risk? It gets more difficult as devices proliferate.

“The solution is a mix of both,” Stoner concluded. “We have to defend the perimeter, the application, and the data.”

Regardless, each customer should develop a comprehensive disaster recovery plan that can restore access to company data in the event of breach, or even in the event that the cloud service provider fails its business and closes its doors with your company’s data behind those doors. These days, Disaster Recovery-as-a-Service has emerged as a viable option that offloads much of the complexity that would be otherwise faced by the end customer. Decision-makers should ask the service provider about “recovery points” that define how frequently data is backed up, and “recovery times” that define how quickly service will be restored, either through the provider’s primary network or supplementary infrastructure. Note that some providers offer more options for recovery points than others.

For more information, contact your Trusted Advisor.

> **“Compliance is not security, and security is not compliance.”**

Compliance

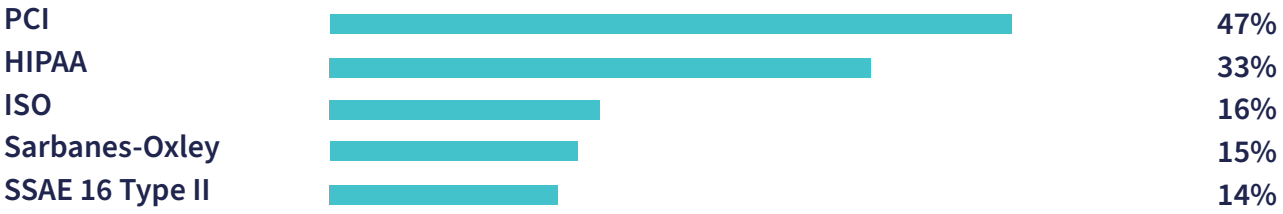
This statement can potentially be attributed to a number of sources, but it has definitely become a widely used trope in the security sector. While security moves too quickly to be effectively codified into a set of requirements that works in all instances, both now and in the future, there is also something to be said for the structure that compliance standards can provide. They are designed to protect the general public as well as the companies forced to adhere to them.

In the United States, the most prominent compliance standards include PCI, which provides regulations around credit cards and other modes of payment; HIPAA, which focuses on medical/healthcare data; and Sarbanes-Oxley, which is designed to preserve the integrity of corporate financial reporting. ISO and SSAE also factor into the equation. In Europe, GDPR has become the de facto standard, and carries serious financial implications for failures to comply.

U.S.-based respondents to AVANT’s assessment survey points to enterprise customers adhering to the following standards at the proportions shown below, based on 197 responses.

Compliance Standard Required

(Based on 197 responses)



Source: AVANT Assesment Data

Even if your company is not required to adhere to a standard, it is often a valuable exercise to choose a standard that can be used as a useful framework for establishing necessary controls and policies.

The "People" Aspects of Security

In addition to technology solutions, most Trusted Advisors are likely to recommend that companies require their employees to attend IT security related educational programs. A number of companies are already requiring such participation on an annual basis, frequently in the form of a third party-designed webinar that focuses on human behaviors such as identifying the characteristics of a likely phishing attack. The extent to which these initiatives are effective can be somewhat debatable, but most experts agree that if they prevent at least one person from plugging-in a USB drive found in the parking lot, then at least some value has been delivered.

"User education is critical to preventing phishing attacks, but you have to assume that you're not going to get 100 percent effectiveness across your entire user base," said Stratacore's Pallat. "The phishers are getting more and more sophisticated, so even a well-educated user can fall victim to a well-crafted spearphishing campaign. So, it's just as important to put some additional email security in place to either sandbox URLs or provide that extra layer on top of what's already available."

While security technologies can go a long way towards protecting your company, a comprehensive education campaign for employees is almost always the necessary next step.

There is one other important "people" aspect of IT security worthy of consideration. While security professionals play a crucial role in protecting the company and its data assets, they are often viewed by their colleagues in a less-than-favorable light.

"There's a battle between the security and the operations people because security tends to make things more difficult, and Operations' goal is to get things done," said Ben Thornton, CTO of Opex Technologies, a Trusted Advisor that specializes in security and other Information Technologies. "The security guys are seen as the "no" guys. So, we try to find out what their concerns are, change that impression and accomplish security goals in less obtrusive ways. This helps to build credibility and good will with other groups within the company. This way, when you do have to say no about something, they don't just try to work around you. They need to see that you have solid reasons.

> **Don't be the "no" person or the "yes" person. Be the "solutions" person."**

Key Action Items

- "Fast cars can go faster if they have good brakes." Approach security as a technology enabler as opposed to a defensive requirement.

- Decision-makers should be willing to answer Trusted Advisor questions about how they respond to specific threats. Doing so will help them help you.

- Place particular emphasis on the collection of supporting metrics, the identification of key areas in need of particular protection, areas in which necessary protection is not provided, and an assessment of specific risks, attack surfaces, and attack vectors.

- Don't focus solely on protecting that single, most critical resource. Attackers merely need to access a vulnerable machine that has access to that critical resource, sometimes via multiple hops. Take a detailed look at how systems are connected.

- Make proactive threat hunting part of your security posture.

- Defend both your data center and your web-based services.

It Happened. Now What?

When a successful attack against your organization occurs, the required intervention must be both human and technological. The great irony of IT security is that, despite your best efforts, some form of successful attack is likely to happen at some point, no matter what you do. After all, defenders have to be right every time, whereas attackers only need to be right once. To further complicate matters, it might not be immediately clear when the actual penetration has taken place.

This is especially true when an advanced persistent threat is successfully launched. After the initial compromise, the attackers will be looking to extend their access to other devices on the network, execute privilege escalations in order to extract more data, and generally move through your infrastructure until they find the specific targets that they seek. Once this is done, they may cover their tracks and withdraw, or more likely they will try to maintain a presence on your network that can facilitate future attacks. Bear in mind that data can be intercepted while in transit or stolen while at rest.

While it makes sense to do everything possible to fend off these attacks and prevent them from happening, it is equally important to assure you have the infrastructure in place to detect the breach, notify the necessary people, and collect all the necessary information to track the breach, close the exposure, and prevent it from ever happening again. Many experts suggest the best tactic is to delay the attacker long enough for the security teams to discover the incursion (or attempted incursion) and resolve the issue before damage is done, or until it can at least be minimized.

This is essentially a team approach that transcends your technologists and engages business-level roles, as well. This team might also include your Trusted Advisor and a managed security services provider, if one has been commissioned. It may also include your communications team.

"Many times, we assume that the most important component to the response to an incident is the technical component, which is let's get the systems and operations back up and running and let's get the impact minimized," said Leo Taddeo from Cyxtera. "I've always believed that the technical aspects of incident response are not as important as the communications aspects. If you look at what really harms a company after a cyber breach, it's not they've lost data or a server. What they have lost is trust, and that trust is lost when communications are not concise, clear, and open. So, when you form a task force for incident response, the most important person in the room is the one responsible for outward communications, meaning what are we going to tell our customers and partners? What are we going to tell the government? The government reaction is much more severe when the government suspects the company is withholding information improperly, and thereby putting other people at risk."

Taddeo added that since most executives are trained to protect the enterprise from litigation and loss of reputation, they often translate that objection to severely limiting public information. But breaches and related issues can rarely be kept under wraps for very long. Sometimes employees may speak too much about what they know. Other times the attackers themselves may discuss their exploits, perhaps on the dark web. All this leads to speculation, some of which might be wildly untrue, yet equally damaging to the company.

Key Action Items (Cont.)

- Adopt a comprehensive solution that gathers log information from a wide array of sources and inputs, and then correlates that data with both known threats and behavioral analysis to uncover threats.

- Ensure you have the infrastructure in place to detect the breach, notify the necessary people, and collect all the necessary information to track the breach, close the exposure, and prevent it from ever happening again.

- In the event of a breach, keep your outward communications truthful and complete. Failure to do so opens you to increased speculation and can bring about higher levels of regulatory intervention.

- In an environment of increased phishing sophistication, add more email security, such as sandbox URLs to help keep you safe.

Key Roles in the World of IT Security

IT Security involves companies serving in a variety of roles that represent different portions of the value proposition. The general categories listed below are not necessarily mutually exclusive Different companies may have different models or may merge different models.
Here are the general categories:

Product Vendors

These are the companies that develop the software, products and solutions intended to protect your data and other assets. You 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 mentioned above, sometimes with a portfolio of vendors to choose from, to deliver a security solution. They are not the developers of the product, although sometimes they may combine different products into a unified offer; perhaps combined with an additional 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 certain options available in their service selection 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.

Consultant/Agent/Reseller/Trusted Advisor

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.