vmware

The Seven Cybersecurity Misconceptions Every CIO Should Dispel

And practical advice on what CIOs should do next

Introduction

You've heard the stories: a large Internet company exposing all three billion of its customer accounts; a major hotel chain compromising five hundred million customer records; and one of the big-three credit reporting agencies exposing more than 143 million records, leading to a 25 percent loss in value and a $439 million hit.

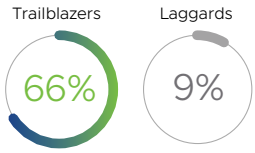
At the time, all of these companies had security mechanisms in place. They had trained professionals on the job. They had invested heavily in protection. But the reality is that no amount of investment in preventative technologies can fully eliminate the threat of savvy attackers, malicious insiders, or inadvertent victims of phishing.

Breaches are rising, and so are their cost. In 2018, the average cost of a data breach rose 6.4 percent to $3.86 million, and the cost of a "mega breach," those defined as losing 1 million to 50 million records, carried especially punishing price tags between $40 million and $350 million.[2]

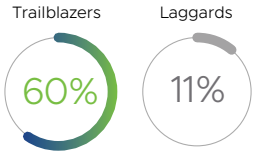
Despite increasing investment in security solutions, bad actors have the resources and the time to poke holes in any enterprise security strategy at any given moment. Unfortunately, it's increasingly not a matter of *if* you will be breached, but *when*.

Areas seeing transformational changes over the last three years[1]

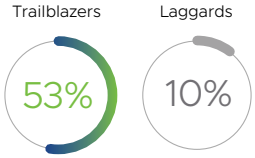
Security Controls
(technology, operations)



Infrastructure
(including cloud, network, compute, storage)



Applications
(architectures, development processes, platforms)



The Cybersecurity Trailblazers

Now for the good news. Do cybersecurity right and you not only better protect your organization, but you're likely to gain a competitive edge in the marketplace.

A recent Forbes Insights security survey of 1,001 global enterprises revealed that 41 percent of "security trailblazers" reported annual growth rates exceeding 20 percent, compared with just 4 percent of their lagging counterparts.[1] These trailblazers are also 10 times more likely to be among the fastest-growing companies, and all share the following characteristics:

- Security teams that are integrated and involved from the start in decisions across the IT technology stack.
- Initiatives such as Zero Trust and least privilege deployed as part of their security strategy.
- Confidence that their enterprise stack—people, processes, and tools—is fully prepared to meet emerging security challenges.

What further set security trailblazers apart was their strategic integration and participation in the business, from sales to the C-suite. These trailblazers consider security a core component of everything the enterprise does, from entering new markets to growing and expanding products and services, increasing revenues, maintaining brand reputation, and improving customer experience. In short, security is *intrinsic* to the business and, furthermore, built into IT infrastructure, applications, and operations.

Debunking the Myths

Most approaches to cybersecurity are still too reactive and too focused on chasing threats. For these reasons, it's critical for teams to rethink security architecture across core infrastructure, applications, users, and operations. For most, changing the paradigm requires investment in new approaches that proactively protect versus proactively prevent. It's equally important to debunk common security misconceptions that prevent enterprise-wide integration of cybersecurity into core business strategies.

MISCONCEPTION NO. 1
A deep understanding of attack trends helps us protect more effectively

Traditional approaches to security are largely reactive. They heavily emphasize processes and techniques to better understand attackers, prevent common-type attacks, and mitigate damage after the fact. But this reactive mode is outdated—if it ever worked at all.

Don't get hung up analyzing attacker motivations or modus operandi. Rather, proactively examine your own environment and identify the apps and data that need the most protection. Understand your workloads and how your users deploy them in the course of their daily jobs. Then give those workloads specific parameters built on the concept of monitoring and enforcing "good" application behavior rather than identifying and mitigating "bad" behavior.

Instead of trying to understand an attacker's intent, focus on an *application's intent, including how an application should behave in its intended state.* Applying security controls based on an app's intended state and behavior is a much more stringent measure of risk and security since any deviations in intended state indicate a threat.

CIO Recommendation: Reduce the attack surface by focusing on an application's intended behavior. Any deviation from an app's specified behavior automatically indicates a threat.

MISCONCEPTION NO. 2
Security is primarily the responsibility of the security team

As data, systems, and applications touch every corner of the business, security should be an enterprise effort led by a spectrum of teams and functions across infrastructure, architecture, network, application, security, and lines of business.

Leading organizations are leveraging DevSecOps models to foster collaboration across development, operations, and security teams in application rollouts. They're also consistently front and center with training efforts that elevate users' knowledge and recognition of common cybercrime techniques. The Forbes security study underscores the importance of collaboration across all IT functions. Unsurprisingly, cybersecurity trailblazers blow laggards out of the water when it comes to levels of collaboration within the organization.

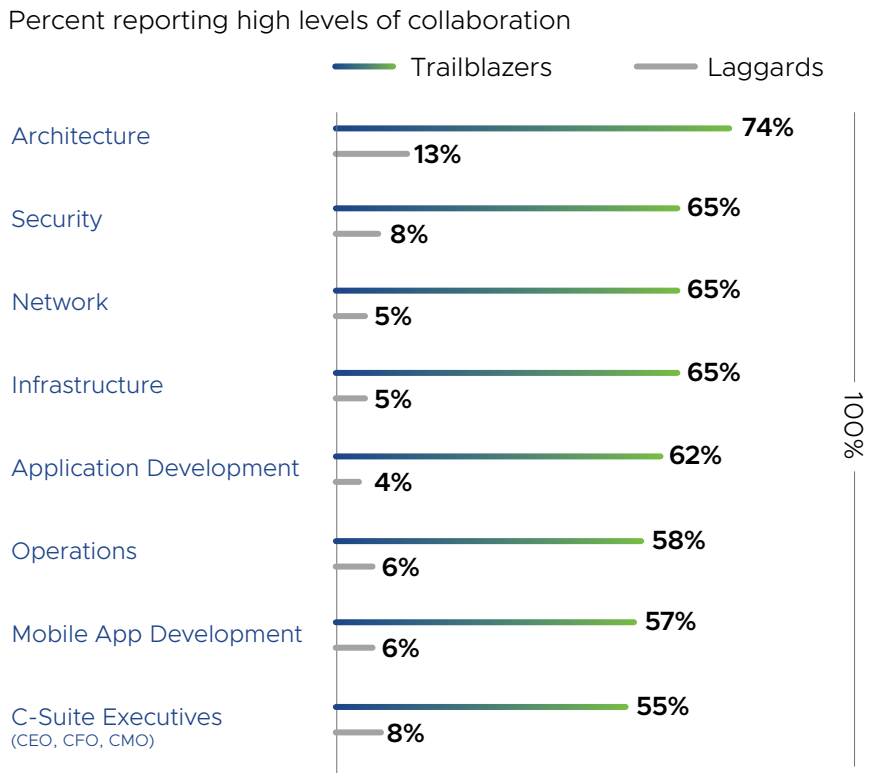


Figure 1: Organizational collaboration in addressing security concerns[1]

Once cybersecurity becomes a collaborative organizational priority, your dedicated security team can concentrate on tasks of higher value, such as testing new security innovations or working with the legal team to interpret and adhere to ever-changing regulatory and privacy laws.

CIO Recommendation: Know that every person in your organization has a role to play in security. Share the responsibility accordingly.

MISCONCEPTION NO. 3
Security teams are the best placed to decide which digital assets to protect

This misconception is widespread. Security teams, despite their technical expertise, need help understanding which digital assets are most critical across various parts of the business. Otherwise, they will attempt to protect everything equally—a costly and eventually fruitless exercise. To them, a database is a database. They don't necessarily know that Database A holds very sensitive customer data, whereas Database B contains the results of historical marketing campaigns. You don't want either compromised, but obviously Database A is more important.

Getting business stakeholders on board is critical. Business partners can identify the digital assets they most depend on and where your organization's crown jewels are—the data and applications that must be protected at all costs. These assets need to be isolated and access tightly controlled so they are used under only very specific conditions.

The concept of Zero Trust is a key part of this approach. With this security stance, an organization operates on the principle of trusting nothing and verifying everything that is trying to access systems inside or outside its perimeters. Zero Trust is generally aligned to the concept of "least privilege," which is a practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities. In an environment of distributed apps, users, devices, and networks, an enterprise-wide focus on a Zero Trust policy for application behavior, devices, and access is critical.

CIO Recommendation: Implement a Zero Trust policy across applications, devices, and users, so the security team can better prioritize resources, introduce stricter safeguards, and set the right policies on the right workloads.

MISCONCEPTION NO. 4
Boards won't approve the necessary budget for security

Boards *will* respond positively to requests for security funds—but CIOs must frame such requests as risk-management exercises that directly impact the business, rather than additional technology investments. Boards are used to managing many different kinds of risk—geopolitical, financial, and market risk. Adding cybersecurity to that list is a logical step.

It's important to explain to the board that no silver bullet exists for cybersecurity. There's nothing you can do that ensures impenetrability except avoiding digital technology altogether. That's not going to happen, so it becomes a risk-management equation. The board will understand your ask for funds in these terms.

Before a board discussion, you'll need to identify the most valuable assets your organization owns. When you meet, you can explain the consequences of those assets being lost, stolen, or corrupted in any way. You can explain the costs—not just the direct costs of mitigating the breach, hiring specialists, buying technology, paying fines and fees, and compensating victims but also the internal resources, such as employee time and attention, that breaches consume. Then there's the biggest but most intangible risk: damaged reputation and, ultimately, revenue loss.

Explain all this in business, not technical, terms and you'll probably get your budget. Indeed, leading security teams stand out in their ability to align security strategies with their board of directors and C-suite.

CIO Recommendation: Frame security spend as a risk-management exercise that directly impacts the business, rather than another technology investment.

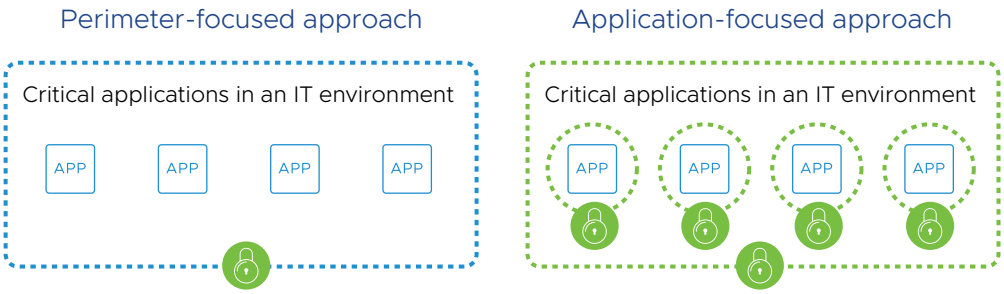
vmware®

MISCONCEPTION NO. 5
Organizations can best secure themselves by protecting infrastructure and the perimeter

Current approaches to protecting data and apps focus on protecting the actual IT infrastructure, like routers or servers. Protecting the infrastructure is necessary, but it's not sufficient. Infrastructure enables an application to operate but is not itself the critical asset to protect. By focusing on protecting infrastructure such as servers rather than the apps or data themselves, CIOs are operating with a disconnected—and flawed—security model.

The reason is this: Traditionally, all application components—including the data—were kept in a single, static server. But with the advent of the cloud, distributed applications, and microservices architectures, app components can be scattered across multiple machines. Point security tools can't distinguish whether a component is used by App A or App B, exactly which components make up App A or App B, or which users should have access to either app.

This is why the traditional perimeter approach doesn't work, and why CIOs should understand the urgency to move to an application-focused security model. Modern applications are distributed and dynamic systems made up of software and hardware components that vary over time. Effective protection moves with the application as it changes.



Additionally, when IT environments are segmented, and the application servers are kept separate from the database servers—which is the traditional approach—you end up with two separate segments, each containing components from hundreds if not thousands of applications. If attackers get through the perimeter protection of either segment, they logically have access to every application in the organization.

A concept called *micro-segmentation* is critical to this point. Micro-segmentation is a security technique in which you logically divide the data center into distinct security segments down to the individual workload level, and then define security controls and deliver services for each unique segment. Micro-segmentation leverages the infrastructure to enable IT to deploy flexible security policies from inside the data center instead of installing numerous physical firewalls.

An even more advanced version of micro-segmentation, *adaptive micro-segmentation*, is now possible. Adaptive micro-segmentation enables you to learn the purpose, composition, and intended behavior of all components that make up an app—both at the network and compute levels; lock down both the workload and network elements; and adapt to application changes in real time.

CIO Recommendation: As IT environments continue to evolve, an application-focused approach to security is not only more effective, but necessary.

MISCONCEPTION NO. 6
Users are your biggest security problem

Many still believe that users are the enterprise's greatest vulnerability, and their susceptibility to clicking on toxic links, visiting dubious websites, or falling for phishing scams leads to the greatest security gaps within the organization.

While sufficient—and frequent—training is still important and necessary, attackers have become much more sophisticated. The reality is that your users can get infected from just hovering over (not clicking) links. Attackers can get into mail servers and send attachments in response to existing email threads from someone a user knows and trusts.

In the old world, where file-based attacks were the norm, user training was a way to solve for that. The reality is that today most attacks (almost 60 percent, according to Verizon's 2019 Data Breach Investigations Report) are file-less and have no download associated with them.[3] They are invisible to users and no amount of training can prevent them. These types of techniques are spreading fast. McAfee identified a 267 percent spike in file-less malware samples in the fourth quarter of 2017 alone.[4]

Then there's the fact that many organizations over-provision access rights to apps and data. In a recent study, 41 percent of organizations had at least 1,000 sensitive files open to all employees.[5] If a least-privilege environment has not been effectively implemented and users are provided with higher levels of access than they need, attackers can steal user credentials and gain broad access to systems. Many companies also don't have safeguards that monitor admin access. Having strong authentication and identity management safeguards in place is a mandate. Identity should be verified using multiple factors, and authentication should be commensurate with the risk of the requested access or function for an individual application.

CIO Recommendation: Although user training is a part of overall security, you should prioritize positioning specific defenses around individual applications by establishing a baseline reference for how an application should operate and who and what needs access when user training fails.

MISCONCEPTION NO. 7
Security by necessity impedes business agility

The security team often has a reputation for being slow to approve new apps or frameworks, and for generally implementing tools that affect performance and productivity.

While most businesses have moved on to Agile software development methodologies, the speed of security review for apps has not increased. Either the app team must put on the brakes—which defeats the purpose of Agile development altogether—or the security team needs to address issues in a timelier manner.

A huge opportunity to jumpstart innovation exists here. With today's automation tools, DevOps teams can push out app updates to the security team in real time. Security teams then perform their review, and push the app out to production. With this method, organizations are actually becoming more agile *because* of improved security.

Here's an analogy: Two decades ago, during heated discussion about improving manufacturing quality, some firms claimed that applying quality measures took too much time and slowed production. They were thinking of quality as an added cost. But it turned out that focusing on quality made manufacturing productivity improve overall. You think you're faster without quality mandates, but you end up paying later. Going back and fixing problems over and over again as opposed to getting it right the first time ultimately impedes progress.

The same can be said about security. You can actually be more agile with robust, intrinsic security because security gets simpler and faster and more effective when you frame it around applications and data as opposed to infrastructure. But this requires shifting your thinking.

CIO Recommendation: Leveraging today's automation tools, DevOps, and Agile methodologies can accelerate security evaluations without affecting app quality or speed to market.

In Summary

Although debunking these misconceptions is a good first step, it is just a first step. Keeping your organization safe from cyberattacks is a never-ending exercise. Enabling the concept of intrinsic security gives you an advantage over attackers, rather than always playing catch up or defense. Breaches are not just costly and bad for an organization's reputation; the CIO also has a reputation—and a job—to lose.

Enforcing security via application behavior is a radical, new approach to security, but it is also complementary to the frameworks that exist today. Intrinsic security doesn't mean abandoning your investment in existing perimeter and endpoint security solutions. It is an *additive* step that makes your security posture considerably more robust.

1 Forbes Insights. "Cybersecurity Trailblazers Make Security Intrinsic to their Business." Joe McKendrick, 2019.

2 The Ponemon Institute. "2018 Cost of a Data Breach Study." July 2018.

3 Verizon. "*2019 Data Breach Investigations Report.*" May 2019.

4 McAfee. "*McAfee Labs Threats Report*." March 2018.

5 Varonis. "*Data Under Attack: 2018 Global Data Risk Report from the Varonis Data Lab: 58% of companies have over 100,000 folders open to everyone.*" 2019.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com