Whitepaper

Building a Strong Cybersecurity Program During IT Transformation

Introduction

Many organizations are in the midst of dramatic changes throughout their data center — as they prepare to transform technology, people, and processes to drive greater agility and service levels by leveraging on-premises and off-premises platforms.

One of the biggest questions as companies set out on this journey is whether they are taking the necessary steps to ensure data security and privacy. The fact is that a lot of large enterprises, as well as smaller businesses, are struggling with where to begin and what to do when it comes to IT security in this new environment.

Unfortunately, getting off to a slow start in building a strong security posture is not an option. Not with attacks growing ever more sophisticated and so much at stake for organizations if they suffer a data breach.

As companies are planning their move to software-defined data centers and hybrid cloud infrastructures, they need to proactively create a cybersecurity strategy that fits well with these newer technologies and IT delivery models.

By deploying the right technology tools and establishing effective policies, organizations of all sizes can develop a security program that will protect all their digital assets, including critical data such as customer information and intellectual property.

This whitepaper examines some of the key challenges IT and security executives are facing as they look to bolster the cybersecurity programs at their organizations at a time when they are transforming their data centers. It offers best practices for building a security strategy that will prepare companies to protect their most valuable information assets as increasingly sophisticated threats loom.

Why cybersecurity is such a struggle

Organizations have long grappled with the difficulties of protecting their data and other IT assets from attacks. Despite heavy investments in technology to secure their networks, data center systems and endpoints, data breaches and other incidents still happen.

Today, the security challenges are greater than ever, with so many organizations making a transition to new data center technologies such as software-defined networks; storage and data centers; hyperconvergence; and all manner of cloud-based services.

Meanwhile, attacks against systems and networks are increasingly more sophisticated and varied, and in many cases, they put companies at financial risk.

For example, in 2016, there were numerous ransomware attacks against companies in a variety of industries. This quickly emerging variant of malware can create havoc for organizations, negatively impacting worker productivity at organizations because users are locked out of their systems until the target company pays a ransom to the attacker.

The number of such attacks worldwide increased sharply through the year, according to multiple industry research reports. Companies of all sizes are being hit with these attacks, and a good number of them choose to pay the ransom.

Other recent trends on the cybersecurity front should be of concern to IT and security executives. One is the ability of distributed denial-of-service (DDoS) attacks to have broad and significant impact. In October 2016, for example, many large and popular internet sites were knocked out of commission after an attack was launched against an infrastructure provider offering managed DNS services. The incident affected users in most of the east coast of the United States as well as data centers in Texas, Washington, and California.

Another development that might present a particularly difficult challenge from a cybersecurity standpoint is the emergence of the Internet of Things (IoT). The prospect of thousands of devices, products, sensors, vehicles, and corporate assets gathering and sharing data via the internet opens up new opportunities for bad actors to hack into systems to steal data or cause disruptions.

Against this backdrop of ongoing and newly emerging security threats and vulnerabilities, many businesses are transforming their data centers to align with their plans to support digital business. They are doing this by deploying technologies such as software-defined networks and data centers and hybrid cloud infrastructures.

Unfortunately, they are also struggling to put in place the right controls for this newly emerging environment. Why is this so difficult for companies large and small and in virtually every industry? There are several key reasons.

It's clear that IT and security executives are facing a daunting array of challenges in building a strong, comprehensive security program for their organizations as they transform their data centers.

Shadow IT

One factor is that when it comes to cybersecurity and technology governance, IT is no longer in the driver's seat at many organizations. The phenomenon of "shadow IT" has been growing for a number of years, with lines of business and even individual departments or groups creating, deploying, and using systems and services without explicit approval from the central IT organization.

Also referred to as "stealth IT," shadow IT can be a source of innovation and agility for companies, because it can enable business users to more quickly acquire the technology they need to improve processes, better serve customers, add efficiencies, etc.

On the downside, however, shadow IT solutions in many cases are not in alignment with an organization's requirements for security, privacy, documentation, and control. The freedom to deploy innovative new systems and applications can leave organizations open to security threats and vulnerabilities that IT and security executives are not even aware of until an incident occurs.

Viewing IT as a roadblock

But the issue goes beyond shadow IT. In many cases, CIOs and other IT leaders are receiving less and less support from business leaders, who view IT as a roadblock. What might begin as a modest shadow IT effort can turn into a situation where business leaders do not consult with IT leadership about long-term technology initiatives within a department or division.

This can create significant cybersecurity challenges if business or project leaders have not taken the proper steps to ensure that corporate data is protected against the latest threats. Oftentimes the problem is not discovered until after a technology effort has already been launched.

This leads into another factor that makes security so difficult in today's business environment. Because there is such an emphasis on speed to market for new applications, products, and services, cybersecurity is often treated as an afterthought.

Despite the constant reminders of the need to safeguard data, the rush to move projects to completion in many cases overshadows the need to deal with the security issues inherent in any new rollout. It's not that business leaders and project teams are deliberately neglecting security; it's more a matter of the competitive pressures of being agile taking precedence over prudence.

IT risk management

Another factor is that many organizations have not defined the degree of risk they are willing to take with regard to cybersecurity. Businesses typically have a good handle on operational risk. For example, a healthcare organization knows in very definite terms the amount of risk it faces from a clinical perspective.

Companies are also quite adept at managing financial risk. Banks know what cases they have on hand and the general financial health of the business at any given time. Companies as a rule have a good handle on capital and how it's managed.

In contrast, many companies have minimal to no handle on how to manage the risks associated with IT and with cybersecurity specifically. They do not extend their risk management programs into the IT and IT security realms. This partly explains why a fancy new app might quickly be adopted — even among senior executives — because of the functionality it provides, without thought of the inherent risks of moving to a new app.

Cybersecurity education

Finally, cybersecurity has been difficult because technology fixes have been the primary focus, with little or no regard for people and processes. Educating and training employees and developing and enforcing stronger policies have taken a back seat.

This gets back to the problem of companies not integrating cybersecurity into the way they do business, making it a part of the corporate culture.

Today, the security challenges are greater than ever.

Building a strong security program

It's clear that IT and security executives are facing a daunting array of challenges in building a strong, comprehensive security program for their organizations as they transform their data centers. But the good news is they can effectively address these hurdles, and if they do they can create a stronger cybersecurity program than they can probably even imagine today.

Before beginning this effort, however, executives need to ask three key questions:

How ready is the organization to make a real effort to improve security, with the full support of executive leadership and the board of directors?

Do all the key stakeholders in the organization clearly understand the cybersecurity risks the company is facing, the risk tolerance of the business, and how it might manage those risks?

Is there a clearly defined strategy around IT security, and what are the objectives of this strategy?

The answers to these questions will help determine whether the company is ready to make an earnest attempt to bolster security. Once that has been determined, enterprises can follow several best practices to help ensure success in building a cybersecurity program designed for the digital business. These practices also address the challenges covered earlier.

First, IT and security executives need to "take back" their organizations from a technology management standpoint.

This does not mean the elimination of innovative technology initiatives within departments and groups. Shadow IT has become a fact of life at many enterprises and the genie is out of that bottle. The proliferation of easily attainable cloud services and the popularity of consumer IT products in the workplace has created a culture of technology freedom within many organizations.

What it does mean, however, is that IT and security management need to work closely with business leaders at all levels of the organization. They must become business partners, brokers of a variety of services instead of obstacles to progress.

That includes helping technology users within the organization in making selections about the best possible product and service solutions, and in ensuring that steps are being taken to make wise choices regarding data security.

Technology leaders also need to make clear that policies are in effect at the company for a reason, and that deployments must be in alignment with the organization's requirements for security, privacy, documentation, and control. At the same time, they need to shake the reputation of being roadblocks to innovation.

If IT and security leaders are viewed as colleagues who aim to enable innovation at the organization rather than as obstacles, they are probably more likely to receive cooperation in making the enterprises safer from a cybersecurity standpoint.

Good cybersecurity practices should be part of the company culture.

To address the challenge of the emphasis on speed to market for new applications, products, and services, IT and cybersecurity executives must find a way to balance marketplace agility with a strong security program. The two do not need to be mutually exclusive.

One thing technology executives can do to get a better handle on this is be part of the early planning cycle with go-to-market initiatives. The sooner they get involved in the process, the better the likelihood of having strong input. Security and technology leaders must be more agile, just as the business has become more agile.

With regard to risk management, it's up to technology and security leaders at organizations to help define the levels of risk associated with cybersecurity specifically. They need to work with senior-level business executives including the CEO and CFO to build a risk management strategy.

These days it should not be too difficult to get buy-in from the highest levels of the organization in creating risk profiles for IT security. The high-profile hacking attacks and data breaches that have occurred at some of the world's best-known companies in recent years has helped bring cybersecurity to the attention of corporate boards of directors. As a result, all business leaders should understand the value of evaluating and managing security-related risks.

And to address the challenges related to people and processes, IT and security executives need to focus on building strong education programs and security policies that address the newly deployed data center platforms.

The importance of training cannot be overstated. Threats and vulnerabilities are changing all the time, and employees and other end users need to be kept abreast of what steps are needed to keep the organization's data safe.

Executives can't assume that everyone knows how to avoid threats. For example, the recent phenomenon of fake news has created new security threats. Some of these sites are being used as a means of launching phishing attacks against companies and individuals. Workers need to know they should avoid clicking on certain links and sharing these with colleagues.

The time for IT and security leaders to start enhancing cybersecurity is now.

As research firm Gartner, Inc. stated in a recent report ("Gartner Threat and Vulnerability Management Primer for 2017," Oliver Rochford, Jan. 24, 2017) a knowledgeable workforce is an essential and consistent requirement of IT security planning. The risk-aware employee is better positioned to limit the business's exposure to intrusion while pursuing business objectives through technology. The leadership must make a commitment to awareness itself: To a campaign of security education and sensitivity, led by the security team and reaching every participant in the business. A security awareness program informs employees and partners what they should do to achieve security and what they should not do.

They should also define and document measurable outcomes from awareness activities that focus on building a knowledge base, complying with regulatory requirements, defining a behavioral baseline, and motivating secure behavior, the firm said. And they should review, build consensus and obtain executive buy-in for prioritized, measurable awareness objectives through one-on-one discussions or group workshops with the stakeholders who are ultimately responsible for the risks that the objectives aim to mitigate.

Good cybersecurity practices should be part of the company culture, with the fact made clear that strong security is the responsibility of everyone in the organization — not just the IT and security departments.

Summary and conclusion

The time for IT and security leaders to start enhancing cybersecurity is now. Cyber criminals, hackers, foreign governments, hacktivists, and others are constantly looking for new and more effective ways to exploit vulnerabilities and attack enterprise systems and networks.

As many companies launch data center transformations and move more data and workloads to the cloud, the security challenges change. But they are still there, and it's up to those running security and IT operations to take the lead on deploying effective technology solutions as well as establishing strong overall security programs.

And the shift in data center technologies and toward cloud services is clearly underway. According to an online survey of 100 IT executives in the U.S. conducted by IDG Research Services in 2016 — and commissioned by Cloud + Data Center Transformation (CDCT) — on average 14% of IT infrastructure and application workload is now in the public cloud, and this will increase to 23% within two years.

IT infrastructure and application workloads in corporate-owned data centers will decrease from 59% to 47% in two years, the survey noted.

The same survey also indicated the importance of cybersecurity in this time of IT upheaval. It showed that security requirements were the top factor among respondents when selecting new IT platforms, with 62% of the respondents saying this was critical.

For those IT and security executives whose organizations are beginning or in the midst of a technology transformation, these are both challenging and exciting times. Failure to implement strong security measures can be disastrous for organizations — and there is virtually no time to spare for taking the necessary steps to protect enterprise data.

By effectively addressing the challenges that many of them face, they can be at the forefront of making their enterprises more secure. That, in turn, will enable their companies to get the most out of these IT transformations.

For more information on our offerings, visit insightCDCT.com.

Meaningful solutions driving business outcomes

We help our clients modernize and secure critical platforms to transform IT. We believe data is a key driver, hybrid models are accelerators, and secure networks are well integrated. Our end-to-end services empower companies to effectively leverage technology solutions to overcome challenges, support growth and innovation, reduce risk, and transform the business.

Learn more at:
insightCDCT.com | insight.com

Insight | Cloud + Data Center Transformation