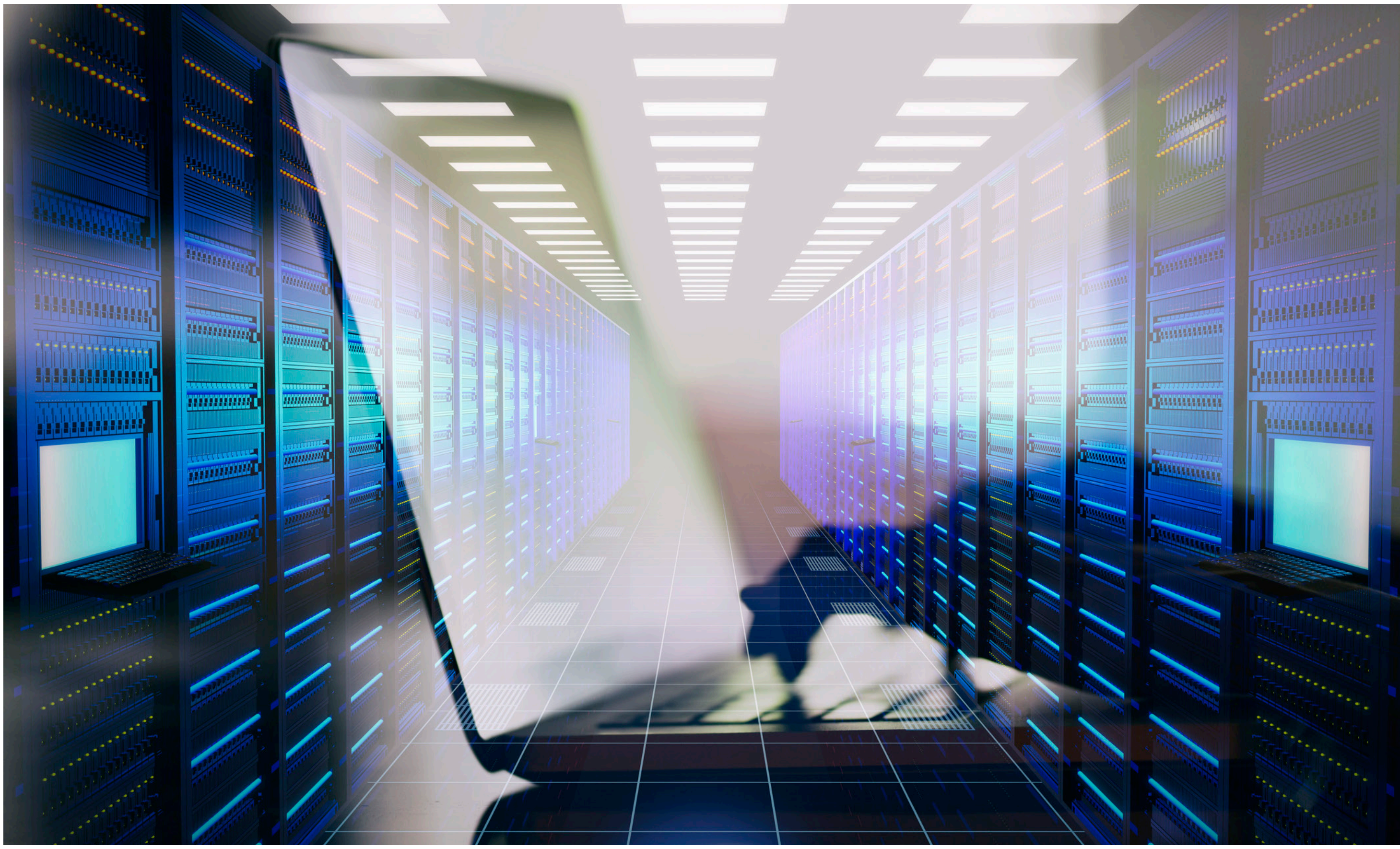
WHITE PAPER

The Cybersecurity Playbook for Midsize Companies



MIDSIZE COMPANIES IN VARIOUS INDUSTRIES WORLDWIDE see increasing cybersecurity protection as one of their top three business goals, according to a new IDG/Cisco survey.

And no wonder. Even as companies face the challenges of an uncertain economy following the pandemic, they are also shifting operations online at an unprecedented rate, introducing a host of new security challenges. More people work at home, for example, and more are expected to stay there, according to McKinsey & Company. Those workers now do the bulk of their work away from the protection of corporate firewalls, often on personal devices, accelerating existing security risks.

Companies also face the twin challenges of deploying new cloud-based technologies while trying to integrate balky legacy systems not designed for the remote work environment (and its security challenges). That's one reason 49% of survey respondents cited legacy systems and siloed data as their top challenge to implementing business goals.

SPONSORED CONTENT

IDG

Clearly, change is not only needed but inevitable at midsize companies. This guide offers best practices for doing just that.

The Cybersecurity Challenge

Today's environment presents unique cybersecurity challenges for midsize companies. These three threats get the top ranking:

1. The rise of ransomware and malware targeting smaller organizations.

In the past, malicious activity and cyberattacks tended to target large organizations—for example, through denial-of-service attacks that took down big company websites.

However, that picture has shifted in recent years as syndicates have arisen to monetize cyberattacks on smaller organizations. For example, ransomware-as-a-service provides turnkey ransomware services to independent operators wanting to profit from holding smaller organizations' data hostage. Encryption schemes promise to unlock data in exchange for payments. Some even include call center support to help victims make payments.

The problem has gotten so bad that the US Federal Bureau of Investigation acknowledges that some organizations may have no choice but to pay up if hit by ransomware. That's because not every organization has the resources to spend millions of dollars to restart operations rather than pay ransom to unlock their systems and data.

2. The need to access everything from everywhere.

The days when most of our work gets done on dedicated devices at the office, on the corporate network, are behind us. Now, users access documents, company databases, and other critical assets on mobile devices anywhere they can get online, including home, coffee shops, public Wi-Fi hotspots, and other potentially insecure locations. The new work-from-anywhere environment makes secure user authentication particularly challenging.

What's more, formerly stand-alone printers, thermostats, photocopiers, and other devices used by businesses now connect to the Internet. And every one of these Internet of Things (IoT) devices can become a target of attacks. As the 2020 Enterprise Security of Things report from Forescout points out, "IoT devices, which can be hard to monitor and control, exist in every vertical and can present risk to modern organizations, both as entry points into vulnerable networks or as final targets of specialized malware."

3. Electronic communications, including emails and instant messages.

Emails and IMs have created streams of data that pour into every company through every device. Those data streams can carry malware, transmit phishing attacks, and more.

All of these factors—already increasing in importance to the threat landscape before the COVID-19 pandemic—became even more acute in 2020. Thanks to lockdowns combatting the pandemic, companies had to expand access to IT infrastructure into homes with almost no warning, before many IT departments were ready.

As a result, security breaches skyrocketed, mainly because companies and their employees had moved outside of policy or security fences that surrounded in-house IT infrastructure. The already-delicate balance between connectivity and security tipped in the wrong direction, revealing gaping holes in company defenses.

Help From the Cloud

The biggest challenge to meeting business goals for midsize companies, cited by 49% of respondents to the IDG/Cisco survey: legacy systems with data locked away in silos. That's even ahead of macro-level environmental factors such as the pandemic and political instability, the second-most-cited challenge. Following that, in third place, midsize companies cited budgets and finances as a top challenge.

Following close behind is the IT skills gap. The shortage is global and not likely to abate any time soon, according to a recent report from the World Economic Forum.

The cloud has the potential to solve at least the top-cited problems that companies can control. That's because the cloud can open data silos, reduce costs, and relieve strained IT departments of much of the burden of IT maintenance. The cloud also has a crucial role to play in the security picture.

Midsize company leaders invest in cybersecurity (at the rate of 46% of those surveyed) more than any other technology type. The only area of technology investment that comes close to security is the cloud, cited by 43% of survey respondents.

Security and the cloud go hand-in-hand. Without the need for on-premises hardware and software that quickly goes obsolete and the associated costs and expertise needed to update and protect them, cloud infrastructure can prove more secure than on-premises data centers, as a McKinsey & Company report notes.

Developing a Strategy

As a first step on the road to greater IT security, midsize company IT leaders should consider security from the beginning when deploying new systems, whether in the cloud or on-premises. Whenever possible, instead of looking at technology in place and asking how to secure it, introduce security as part of initial design requirements.

For example, consider how many users will regularly work at home and how many will be on the road versus on-premises—and design a security strategy from there.

As part of that process, IT departments can assess what stand-alone security applications—and for what specific purposes—to deploy. The goal here should be to make security application deployments judiciously rather than throwing everything available at them.

Recent research by IDG found that enterprises maintain an average of 19 different security technologies—and that more is not necessarily better. Too many applications actually interfere with the security function, as understaffed IT departments struggle to corral and make sense of data from the different sources.

For remote workers, experts recommend making crucial hardware investments where necessary rather than letting employees fend for themselves. "Replace some of your employees' home routers," advised workplace expert Antonio Vieira Santo in a recent IDG TechTalk on Twitter. "There are plenty of devices at people's homes [that] have never been patched. One device can create a liability."

Next Steps

With a strategy in place, it makes sense to turn next to user authentication. Passwords represent the biggest potential pitfall when approaching security because they are the most-exploited attack vector for cyberattacks.

Instead of relying on passwords, the most secure IT infrastructure requires multifactor and passwordless authentication to grant access. That means, for example, opening a mobile application to confirm a login or clicking a secure link instead of—or at least in addition to—entering a password.

That's because even the most difficult-to-remember and frequently changed passwords are vulnerable to attacks on the servers storing them. Multifactor authentication, on the other hand, provides additional authentication methods to block attacks.

After getting the password problem under control, successful security organizations can prioritize tackling the problem of malicious websites. These sites launch attacks when unsuspecting users visit them, typically through an email link sent as part of a phishing attack that tricks users into clicks or malware downloads.

And, to help alleviate the problem of the skills shortage, look to outside vendors to provide needed expertise and extra help.

For example, third-party vendors can provide secure remote work bundles that include, as part of an integrated whole:

- **Authentication**
- **Secure access to company networks**
- **Email protection**
- **Secure collaboration tools**, such as encrypted phone and video conferencing.

Secure conferencing tools take security a step beyond securing data, since they also secure communications between people within and beyond organizations to ensure the confidentiality and integrity of proprietary conversations.

The Bottom Line

Never has there been a more challenging time for cybersecurity, particularly for midsize enterprises. The work-from-home environment, growing numbers of attackers, and an IT skills gap all threaten to create a perfect storm of threats. Even so, cloud architectures, security-first strategies, and best practices can go a long way toward security that can help midsize enterprises meet any challenge.

Learn how the cloud can help secure your organization by exploring Cisco's SaaS solutions for midsize organizations.