IDC ANALYST CONNECTION

Sponsored by: Comcast Business

Midsize businesses face the dilemma of increased cybersecurity threats, complexity in their IT environments, and often a dearth of security skills. An integrated suite of solutions, provided by a trusted provider, is an effective approach.

Using Integrated Solutions to Address Cybersecurity Challenges in Midsize Businesses

September 2021

Questions posed by: Comcast Business

Answers by: Duncan Brown, Vice President, Enterprise Research

Q. What specific challenges do midsize businesses have when it comes to cybersecurity?

A. The first question is, What is a midsize business? There is no agreed-upon definition, and most business executives understand where they sit in terms of the relative size of their business. A defining characteristic might be that the firm has a degree of complexity in its IT architecture beyond that of a small business, but short of that typical of a large enterprise. This complexity can present as a proliferation of IT systems supporting many aspects of the business, which in turn can create security challenges in terms of protecting a variety of systems, platforms, and technologies across a distributed workforce.

Many midsize businesses will have a dedicated IT function but are much less likely to have specialist security resources; therefore, cybersecurity skills deficiencies can be prevalent. It's also not always clear who has responsibility for security, including the day-to-day operations of a variety of security tools. Security should be a primary concern for all midsize business executives, but it often does not get the attention, time, and resources it needs.

A key perception of security is that it adds yet another layer of complexity for companies that value speed and agility; thus, it may become deprioritized deliberately in favor of nimbleness.

Q. What kinds of security threats should midsize businesses be particularly aware of?

A. Many midsize businesses will think of ransomware when they consider security risks. Indeed, ransomware is a growing and particularly destructive threat: It can combine the interruption of business continuity with the prospect of (possibly catastrophic) data loss and the financial consequences of paying a hefty ransom. Other factors to add to this equation are the reputation damage caused by such an attack in addition to the resources diverted from usual business activities to try and deal with this disruption.

Ransomware is not the only form of security risk. Most attacks try to steal user credentials as a first step and then attempt to extract data that can be misused or sold. A dimension of this approach is to steal deliberately targeted intellectual property (IP) that can be either sold to competing firms or simply copied. The potential damage that this type of attack can inflict is substantial. Credential theft can also be used in business email compromise (BEC) attacks, whereby an illicit request for a payment or funds transfer appears to come from a legitimate source. The money is often paid to the attacker unwittingly, and the payment is discovered only after the fact.

Ultimately, firms of all sizes are subject to security risks, but midsize businesses are particularly vulnerable because they are often attractive targets to attackers and possess fewer means to defend against such threats.

Q. How can IT leaders demonstrate the business value of cybersecurity?

A. Cybersecurity can quickly focus on the technical aspects of the subject. This can often mask its business value. One positive effect of the pandemic is the broad realization that security can help enable business. As many organizations migrated their workforces to home or other remote environments, as well as accelerated their migration to the cloud, traditional security approaches needed to be adapted to accommodate these new architectures. In general, this adaptation occurred relatively smoothly and resulted in a recalibration of the value of security.

Security technology and nomenclature may be technical, but security outcomes can be expressed in business terms in a straightforward manner. Rather than emphasize a security approach that involves specific products or solutions, you should identify the sources of business risk and state the desired outcomes. For example, your manufacturing facility must maintain availability. Your customers' data must be protected. Unauthorized or illicit demands for payment should be detected — and so on.

It is important to tailor security solutions to your business. Think about ease of implementation, integration, and administration as core elements of any technical solution you are considering. These elements may seem trivial in comparison with the technical features of any given product, but if you get them right, you could save time and money while operating such solutions. It may also be preferable to buy a bundled suite of solutions from a single vendor rather than a disparate array of point products.

Q. What is a good way for midsize businesses to increase their cybersecurity skills and maturity?

A. As previously noted, security can get complicated very quickly. Given that many midsize businesses also don't have a deep pool of security expertise at hand, it's important to engage with other parties that can help you through the process. Plenty of free — and expert — advice is available from the following organizations, among others: The National Institute of Standards and Technology (NIST) produces standards, guidelines, and best practices for security; the Cybersecurity and Infrastructure Security Agency (CISA) coordinates security and resilience efforts for the nation's cyber and physical infrastructure and produces security advisories and recommendations; the SANS Institute is a for-profit company that specializes in information security, cybersecurity training, and security skills certification.

Above all, you may not want to try to fix all of your security issues at once. Prioritize the critical business systems that you depend on, and choose a technology provider to assist you as you go.

Q. What should midsize businesses look for in a technology partner?

A. Midsize businesses should engage with a provider of cybersecurity solutions for midsize companies. Such partners will have the scale to accommodate a wide variety of technologies and IT environments and will have the depth of expertise to cope with the degree of complexity typical for a midsize business.

An integrated suite of solutions that span not only cybersecurity but also networking solutions can help simplify administration and vendor management. Partners that can deliver such an integrated solution can help free up some of your resources, allowing you to focus on core business activities.

A wide variety of services are available: Select a partner that can help pick the right solutions for you and can also provide the customer support you need.

Choosing a provider that you can trust is important. You should select a provider that will help alleviate the burden on your IT department. A good partner will get to know your unique business needs and design solutions that fit those needs. The more you engage with that partner, and the more that partner can provide an integrated suite of capabilities, the better it can be for you.

About the Analyst

Duncan Brown, *Vice President, Enterprise Research*

Duncan Brown specializes in providing strategic advice to his clients, informing and validating their corporate, product, and marketing plans. His analysis and opinions are widely sought by industry leaders and investors, while his comments on industry trends and developments frequently appear in the leading business and trade publications. Brown started his career in the banking sector; most recently, he spent time as Chief Security Strategist on the vendor side. He is a well-known and respected analyst with IDC customers.

MESSAGE FROM THE SPONSOR

Comcast Business Secure Network Solutions

Comcast Business now offers secure network solutions, combining our nationwide SD-WAN with new UTM security solutions from Versa and Palo Alto Networks to offer integrated on-premise and cloud solutions to help protect your network. Our secure network solutions are powered by ActiveCore, a one-of-a-kind digital platform, that makes it easy to access real-time insights and control your network from anywhere.

Learn more here.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.