An InteliSecure Whitepaper

InteliSecure

ADVANCED DATA PROTECTION NOW WITHIN REACH FOR MID-MARKET COMPANIES

Robust security programs are more accessible, affordable, and capable than ever before, helping confront a deluge of new regulations and cyber threats

CONTENTS

Old Excuses

While most mid-market companies have conventional firewalls and intrusion detection products in place, countless others have eschewed more robust security solutions and services. And they've justified their hands-off approach with a variety of misconceptions and excuses.

Some mid-market executives assume their company isn't a target, believing hackers and the malware they wield are aimed at high-profile corporations and government agencies. Many have come to the conclusion that advanced security is financially out of reach, built for the largest of enterprises with the deepest of pockets. Others are wary of the time and resources it might take to fortify their defenses, and the complexity and learning curve they would presumably endure.

But such notions are no longer accurate, and mid-market companies can no longer neglect their most critical data assets. Not with a host of new laws and regulations that now apply to organizations of every size. Not with a level of risk that is actually higher than large enterprises face.

Fortunately, robust security programs and services are now within reach for every company.

New Requirements

Many countries are enacting increasingly stringent laws for data protection and privacy, and they're not just aimed at large corporations.

The new General Data Protection Regulation (GDPR), for example, is a major piece of legislation that will affect EVERY organization that handles user data and has dealings in the EU, according to IT Pro. The key points of the legislation are that businesses must have full consent and an opt-in from the user that cannot be confusing. For instance, a company must state precisely what data is being collected, what it will be used for, and how long it will be stored. And if a business wishes to use the data for purposes outside of the original opt-in, they must seek permission from the user before it can happen.[1]

GDPR has set a comprehensive and daunting standard for organizations large and small. And many countries

[1] *http://www.itpro.co.uk/data-protection/29123/gdpr-for-small-businesses-what-it-means-for-you*

outside Europe are following suit with similar requirements. The U.S. has fundamentally different privacy models, many of them focusing on industry sectors. Health information is regulated under HIPAA, for example. Financial information is regulated under GLBA and FCRA. And marketing falls under the TCPA, TSR, and CAN-SPAM regulations. To further complicate matters, U.S. states like California are now enacting their own privacy laws.

Navigating these differing philosophies and regulatory models—not to mention a complex matrix of distributed customers, employees, and data—can be extremely difficult for every company, but especially those that are unaccustomed to broad and multifaceted compliance mandates.

All companies, regardless of size or location, must now be keenly aware of the user data they collect, where it originated, how it is transported and stored, and when it crosses borders.

LEXOLOGY: DATA PRIVACY POLICIES AND PROCEDURES NOW MANDATORY

Companies that may not be used to operating under strict regulations will now have to adopt and develop new policies, procedures, and compliance mechanisms. Companies will have to understand what personal information they collect and use from foreign citizens, whether they are employees or customers. And they will have to ensure they have a compliance program to satisfy new requirements to properly and safely transfer such personal information.

https://www.lexology.com/library/detail.aspx?g=4b2843f7-f67a-4015-bca9-96bd2fe344c9

Greater Risks

Cybersecurity threats, data breaches, and the problems they can create for organizations have been well chronicled. But few realize the risks are greater for small and mid-sized companies.

Large enterprises typically have more robust security systems and processes in place than mid-market organizations, allowing them to quickly identify an attack or breach and minimize the damage. And when those safeguards fail, they have the resources—spanning finances, internal staff, and external service providers—to deal with the crises that often follow. They have the armor to protect their most valuable assets and the ability to recover if those assets are compromised.

Conversely, a cyber attack or data breach can put a small or mid-sized company out of business. Many mid-market organizations can't afford to get dragged into court, pay significant regulatory fines, hire a publicity firm to repair their image, lose a percentage of their customer base, or patch up the technical vulnerabilities that were exploited in the first place. And modern security events often involve all of them.

The Silver Lining

Despite daunting regulatory requirements and considerable risks, there is indeed a silver lining: Advanced security solutions and services are now within reach for every mid-market company.

The notion that world-class data protection is too expensive, too complex, and too resource intensive for all but the largest of enterprises is no longer accurate. Software solutions are more capable and affordable than ever before. The flexibility and on-demand accessibility of cloud resources have removed the burden and cost of building or retrofitting data center systems to fortify an organization's defenses. And managed security service providers (MSSPs) can bring a wealth of experience, methodologies, and economies of scale to the table, helping mid-market companies assess, prioritize, and optimize their security spending and data protection. In fully managing a security program, MSSPs are able to reduce overall security costs as well as the time to incident identification and remediation. And their experience working with companies of all sizes across a number of industries can be readily applied to mid-market needs and budgets.

CRITICAL DATA ASSETS DEFINED

A critical data asset is any piece of information that could cause irreparable harm to an organization should it be lost, stolen, improperly shared, or improperly exposed. Some types of critical data are well known and regulated pieces of information, such as Protected Health Information (PHI), Personally Identifiable Information (PII), and Payment Card Industry (PCI) data. Other types of critical data aren't regulated but are very important to a company, such as intellectual property, business research and planning information, financial statements, price lists, and merger and acquisition details.

At the end of the day, information security is all about balance—of cost and risk.

Because budgets and resources are always limited, there is no way to fully protect everything at all times. Experienced security services companies can help identify an organization's most critical data assets and vulnerabilities, and then shift resources to the areas of greatest risk. In doing so, they enable mid-market organizations to get the most benefit for the least cost.

Summary

In an era of precarious and dynamic business risk, advanced data protection is no longer a choice for mid-market organizations. The laws are unbending, the threats are unrelenting, and the consequences can be catastrophic if they are not confronted with a rock solid security program.

Fortunately, these programs are more accessible, affordable, and capable than ever before. MSSPs can help identify and prioritize the assets of greatest value to a mid-market organization. They can conduct business-focused threat assessments and redirect security dollars to the areas of greatest risk. They can design and implement programs that provide the most protection for the least cost. And they can manage and optimize those programs over time.

Excuses and procrastination won't keep regulators or hackers at bay. For every mid-market organization, now is the time to re-examine, re-balance, and fortify their data protection capabilities.

About InteliSecure Managed Security Services

Perimeter-only security programs continue to be ineffective against today's persistent threats.

That's why InteliSecure, unlike traditional MSSPs, is laser focused on protecting your most critical data assets—based on revenue, income, reputation, and core operational impact—at the perimeter and everywhere else.

Combining people, process, and technology, InteliSecure's proven Critical Data Protection Program™ methodology safeguards your most sensitive assets from malicious and accidental breaches, whether from external or internal sources. The result is a more targeted and effective security posture.

To learn more, visit www.intelisecure.com.

INTELISECURE INDUSTRY FIRSTS

- One of the first 10 organizations recognized as an ISO 27001 Associate Consultant by the BSI Group (2006)
- First MSSP to offer managed DLP services (2008)
- First MSSP to combine machine data with heuristics-based analytics for content and context based approach (2008)
- First MSSP with a focus on critical asset protection programs across all services—data and threat protection (2013)