866-726-4271
info@idexpertscorp.com

WHITEPAPER

Calculated Risks: Data Breach and the Mid-Market Company

Running a mid-market company is an exercise in calculated risks: Can you grow the business without over-extending? When do you invest in new technology? How do you prioritize spending when every dollar counts? The challenge is to calculate the opportunities and risks correctly and spend strategically.

Some of the biggest emerging risks for the mid-market are those from data breaches. The data security and privacy landscape is changing quickly, and many mid-market companies are just beginning to recognize the risks they now face, risks that no business can afford to ignore.

The new reality is that data breaches are inevitable. The majority of businesses now hold some form of protected information, and with businesses moving to cloud services, mobile computing, point-of-sale systems, and information-sharing with business partners, that information is more exposed than ever. Cyber-criminals are now targeting businesses of all sizes, and a new cyber-risk handbook from the National Association of Corporate Directors states the case bluntly: "If a sophisticated attacker targets a company's systems, they will almost certainly [be breached]."[1] At the same time, regulatory requirements and litigation risks around data breaches are also growing.

And while businesses of all sizes and across all industries now face the constant threat of data breaches, mid-market companies face unique challenges in planning and responding to breaches. Business leaders in the mid-market (companies with revenues between $10M and $1B) need to spend strategically but also responsibly, and in today's threat climate, to be unprepared for data breaches is literally to bet the company.

The New Cyber-Security Landscape

Even a decade ago, no one would have predicted the kinds of data breaches that have become commonplace today. Cyber-crime, cyber-terrorism, and cyber-espionage are rampant, and the data is sold on black markets and exploited often within hours.[2] Yes, the breaches that make headlines affect millions of users, but size is no longer the main factor that determines the seriousness of a breach. Mid-market companies may not have hundreds of millions of customers to protect, but they now face the same risk factors as larger organizations.

Expanded Data Equals Expanded Risk

Information technology continues to revolutionize business: social media extends our marketing reach, cloud computing lowers IT costs, business analytics guide strategy, and smartphones and tablets enable everything from the mobile workforce to mobile payments. However, each new destination and conduit for digital information is also a new potential point of attack. Customer databases, analytics, social media, and mobile computing have created a massive expansion in the amount of personal

> "In between all the hyped stories about military-grade malware like Stuxnet and Flame, business executives miss the real threats to their business — cybercriminals are targeting your intellectual property and customer data, and an erosion of customer confidence in your brand kills your ability to win, serve, and retain customers."
>
> - Forrester Report: "Protect Your Intellectual Property And Customer Data From Theft And Abuse." July 10, 2015

information that is held by businesses of all sizes and exposed via the Internet. Digital integration with business partners has also been a boon, affording businesses access to on-demand services and expertise, and enabling the growth of business service companies. But a chain is only as strong as its weakest link: the security of an organization's data now depends on the security of each partner which whom that data is shared, and a recent study by global consulting firm Protiviti and The Shared Assessments Program found that vendor risk management programs across industries rate an average of 2.8 on a maturity scale of 1 to 5.[3]

Cyber-Crime on the Rise

A decade ago, the most common causes of data breaches tended to be a lost laptop, insider theft, or identity theft by small-time criminals. Now studies show that the majority of data breaches are the result of sophisticated cyber-attacks.[4] And while financial fraud is still the most common motivation for malicious breaches, it is dropping fast in relation to extortion, cyber-espionage, and other attack motives.[5] Ransomware is a fast-growing, multimillion dollar business that is being used against everyone from individual consumers to government agencies. Data theft can also come through common business software. Attackers are now spreading malware through software updates,[6] and security firm Kaspersky discovered that a cyber-attack called "Red October" has been exploiting Microsoft Word and Excel vulnerabilities to steal data from companies of various sizes since 2007.[7]

> "Thirteen years after California passed the first-ever breach notification law in 2002, there are now only three states that do not have one — Alabama, New Mexico and South Dakota. While most states have embraced the need for consumer identity theft remedies and notification legislation, there are almost as many differences in each state's law as there are states."
>
> – Elizabeth C. Rogers, Law360[10]

In fact, many mid-market companies are prime targets for cyber-crime because they don't have budgets for high-priced security systems or dedicated security staff. The 2015 Verizon data breach report found[8] that while large companies reported 70 times more security incidents than smaller companies, the percentage of incidents that turn out to be actual breaches is probably consistent regardless of company size. And since more than half of data breach victims are small to mid-sized companies, the fact that large companies report more security incidents suggests that mid-sized and smaller companies are less likely to track incidents and are only finding out about them after they become data breaches.

Less to Spend, More to Lose

Just as mid-size businesses face the same security risks as larger companies, they also face the same kinds of business risk when breaches happen. The difference is that most mid-sized companies have smaller budgets and fewer resources to deal with the problems, so the consequences of a serious data breach can potentially cripple or sink the business.

The Regulatory Maze

As cyber-threats mount, so do regulatory requirements. A complex maze of federal and state regulations impact businesses that hold any kind of protected personal information (PPI), and a survey by The Hartford found that 81% of mid-market businesses report storing this kind of sensitive data.[9] Today, businesses that don't comply with regulations can face multi-million dollar penalties, and while a large corporation may be able to absorb those fines as a cost of doing business, costs of that magnitude can seriously damage a mid-size business.

New Litigation Risks

In addition to regulatory risks, breached organizations are facing new risks from litigation: data breach victims are now bringing lawsuits and winning. For example, in July 2015, the 7th U.S. Circuit Court of Appeals reinstated a class action lawsuit against retailer Neiman-Marcus over a 2013 cyber-attack,[11] and UCLA Health System became a defendant in a class action suit over a breach of patients' personal data and medical records.[12] In 2014, Stanford Hospital and Clinics settled a class action suit for $4.1 million, online ticket seller Vendini created a settlement fund of $3 million in a suit for breached credit card numbers, and social media networking site LinkedIn settled a suit for $1.5 million.[13] In industries that hold particularly sensitive information, such as finance and healthcare, settlements in even individual identity theft cases could run to millions of dollars, enough to put a mid-size company out of business.

Loss of Business

In addition to the potential for regulatory penalties and lawsuits, data breaches can damage business relationships with customers, and mid-size companies can be even more vulnerable to revenue loss and more dependent on customer trust. Consider a mid-size retailer, legal office, or financial firm that serves high end clients, or a property management company that serves property owners and renters. If personal information is breached and clients leave and tell friends and colleagues, businesses like these might never recover. Likewise, a business that provides services to larger

companies can't afford to lose the data of its business partners. Not only could the client companies end the business relationship, they might also hold the services provider legally responsible for their damages and damages to their customers.

Cyber-risk Readiness in the Mid-Size Organization

Mid-size businesses face the same risks as larger ones, but they face greater challenges in dealing with cyber-crime. In the findings from its 2015 State of Cybercrime Survey, PricewaterhouseCoopers notes that mid-sized companies[14] are less likely to have invested in information security staff and programs over the years, and as a result, they detect 60% fewer incidents than larger companies.[15]

Mid-sized and smaller companies are at a disadvantage for hiring information security staff. In a recent interview with ISMG, security expert Stuart Itkin noted that of the 100,000 new U.S. engineering graduates per year, only about 3,000 have security credentials, and those high-priced individuals are snapped up by larger organizations.[16] He also cited a recent survey which found that a third of mid-size businesses don't believe they are targets for cyber-attacks, yet the 2015 Symantec Internet Security Threat Report found that 60% of all attacks targeted small and medium-sized businesses.[17] Incidents detected by mid-size companies in the past year have led to an estimated financial lost of $1.8 million per company.[18]

Mid-size companies need to prepare for the inevitable breach incidents by putting in place processes and locating outside vendors who can provide breach assessment, notification and identity protection when needed. The mid-size business study by The Hartford[19] found that 82% of mid-size organizations see data breach as a risk and 32% of them see it as a major risk, yet a recent Forrester report found that, even at those enterprises that had suffered a breach during the past 12 months, only 24% reported increased spending on their incident response program as a result.[20]

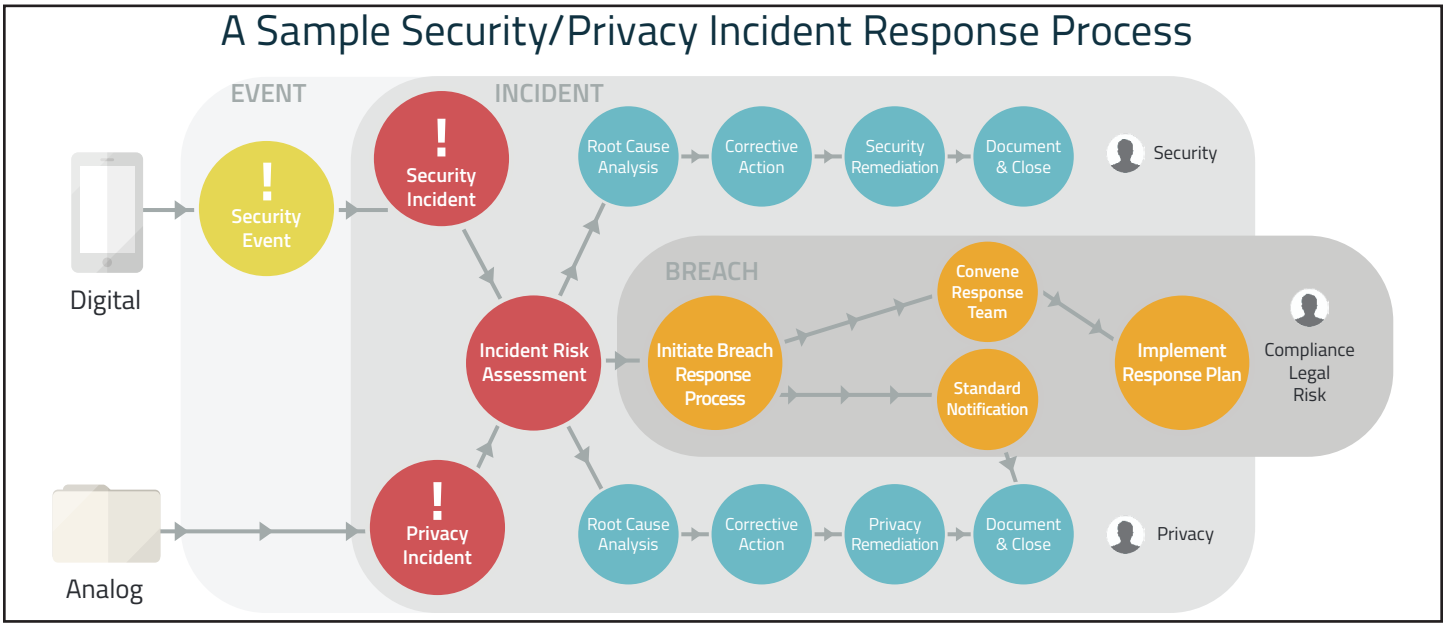
> "As larger quantities of diversified data are amassed on a range of devices and third party service providers are increasingly relied upon, every business must be prepared for the inevitable loss of data."
>
> – Online Trust Alliance 2015 Data Breach Protection and Readiness Guide.[21]

Most breaches at mid-size businesses aren't as large as the ones that make national headlines: on average, there will be from 1,000 to under 100,000 people affected. However, the data may be just as sensitive and the compliance risks just as severe as in breaches affecting larger companies. Fortunately, today's escalation of data breach risks coincides with a recovering economy that will allow businesses to begin investing in data breach preparedness.

Inaction is Not an Option

Risks to your information and your business are mounting, and therefore so is the cost of not taking action to meet those risks, especially for mid-market organizations. Data breaches can sink a business, and they can sink management careers. Given the risks, the costs of preparing for and responding to data breaches are not only manageable, they are critical to the well-being of the organization.

A Sample Security/Privacy Incident Response Process



The key steps are to understand your risks, create an incident response process, and retain a partner that can handle, at scale, all phases of breach response.

Assessing your risks in today's cyber environment is critical to protecting your organization. In the process, you identify what data you hold, where it lives, in what forms, and the risks of misuse, as well as the regulations that apply to your business. It will tell you what data is most vulnerable, what data sets are most likely to be targeted for cyber-attacks, and where your organization might be a stepping stone in an attack on a business partner. The results of a thorough risk assessment will help guide you in addressing cyber risk. Obtaining insurance may be a part of the solution, but it can't be all of it.

> "Protecting data — be it customer, employee, or company — is a corporate social responsibility and is vital to an organization's continued success and growth."
>
> – Forrester Report: The Cybercriminal's Prize: Your Customer Data and Competitive Advantage

Next, you need to develop and implement an end-to-end incident response process. A 2015 PriceWaterhouseCoopers security survey found that the number of detected incidents soared to 42.8 million in 2014,[22] so it's clear that security incidents are happening all the time, whether they are being detected or not. For most businesses, numerous incidents are happening every month. Each incident is a potential data breach, depending on whether it qualifies as a breach under federal and state regulations, and each carries risks of regulatory penalties, lawsuits, and lost business if not handled correctly. You need a consistent, repeatable process for managing incidents on a day-to-day basis, to be able to quickly identify and address root causes, determine the risks from each incident, assess the extensive web of federal and state breach notification laws, and document your findings and actions to meet regulatory requirements and to be prepared for possible future litigation. Your information security and privacy/compliance staff needs to practice incident response as an operational process. Incident response software can help them to collaborate, quickly pinpoint risks specific to the incident, and document the findings and decisions to help with compliance.

When an incident is classified as a data breach, your ability to carry out a timely and compliant breach notification and response depends on having the right team in place ahead of time, including your internal team and your trusted partners. If you're not a large enterprise with dedicated response staff, your corporate counsel may not have expertise in data breach notification laws and regulations. Many mid-market companies also lack internal data forensics expertise. And very few companies, independent of size, have the ability to quickly staff a specialized call center, mail thousands to millions of specialized letters, or provide an identity monitoring solution to breach victims. Notification needs to be done quickly, and it needs to be done right, so retaining a trusted partner with these specialized capabilities is critical.

Given the speed at which threats, regulations, and legal precedents are evolving, most organizations are well advised to rely on their breach response partner to stay on top of the cyber-breach world for them. Between the specialized knowledge needed to determine compliance requirements and the critical and typically short regulatory timelines for breach notification, the most practical and cost-effective way to prepare is to have a breach response partner on retainer.

Running a mid-size business involves making hard choices, but in the case of data breaches, there is no choice. These are simple steps that no organization, regardless of size, can afford not to take.

Get Started Now

ID Experts offers the most complete breach response services available today and is the only breach services provider focused on serving the needs of mid-market companies. Our team provides vital expertise and staffing for incident response planning, and all phases of breach response, including digital forensics, breach determination, individual and regulator notifications and consumer identity monitoring and recovery. We look at breach response through the lens of the risks to our clients and to the breach population, matching the response to the risk profile of the incident to deliver both cost-effective breach response services and maximum protection to our customers and their customers.

Get started now with ID Experts and retain us as a trusted partner. Research our breach response products and services by visiting www2.idexpertscorp.com/data-breach-response or call 971-242-4775.

End Notes

1 Clinton, Larry. "Cyber-Risk Oversight Executive Summary." Director's Handbook Series published by the National Association of Corporate Directors, 2014.

2 Verizon 2015 Data Breach Investigations Report. http://www.verizonenterprise.com/DBIR/2015/

3 2015 Vendor Risk Management Benchmark Study. http://www.protiviti.com/Pages/Protiviti-VRM/index.html

4 Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data. Ponemon Institute, LLC: 2015.

5 Verizon 2015 Data Breach Investigations Report.

6 http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/

7 http://rt.com/news/red-october-cyber-attack-network-000/

8 Verizon 2015 Data Breach Investigations Report. http://www.verizonenterprise.com/DBIR/2015/

9 The Hartford. 2014 Midsize Business Monitor. http://www.thehartford.com/midsizemonitor

10 "Top Tips For Data Breach Readiness And Response." March 25, 2015. http://www.law360.com/articles/634505/top-tips-for-data-breach-readiness-and-response

11 http://blogs.reuters.com/alison-frankel/2015/07/21/the-7th-circuit-just-made-it-a-lot-easier-to-sue-over-data-breaches/

12 http://www.natlawreview.com/article/class-action-suit-filed-against-ucla-after-it-suffers-massive-data-breach-affecting-

13 http://www.wsandco.com/about-us/news-and-events/cyber-blog/cyber-cost

14 Defined as companies with between 1,000 and 3,000 employees

15 U.S. cybersecurity: Progress stalled. Key findings from the 2015 U.S. State of Cybercrime Survey, PwC, July 2015. The 2015 US State of Cybercrime Survey was co-sponsored by PwC, CSO, the CERT® Division of the Software Engineering Institute at Carnegie Mellon University, and the United States Secret Service

16 http://www.databreachtoday.com/mid-market-security-challenge-a-8135

17 Symantec. 2015 Internet Security Threat Report, Volume 20.

18 PricewaterhouseCoopers, CSO Magazine, CIO Magazine. The Global State of Information Security Survey 2015. September 2014.

19 The Hartford. 2014 Midsize Business Monitor. http://www.thehartford.com/midsizemonitor

20 Forrester Report: Planning for Failure. May, 2015.

21 https://otalliance.org/system/files/files/resource/documents/dpd_2015_guide.pdf

22 "PricewaterhouseCoopers, CSO Magazine, CIO Magazine. The Global State of Information Security Survey 2015. September 2014.

Talk to an Expert

971-242-4775

Info@IDExpertsCorp.com

Learn more online

www.IDExpertsCorp.com

@IDExperts

All Things HITECH
All Things DataBreach

About ID Experts

ID Experts® provides software and services to simplify the complexities of managing privacy and security incident response. For more than a decade, ID Experts has provided data breach services and managed thousands of incidents. ID Experts is an advocate for privacy and participates with the Consumer Federation of America, the PHI Protection Network and Patient Privacy Rights.