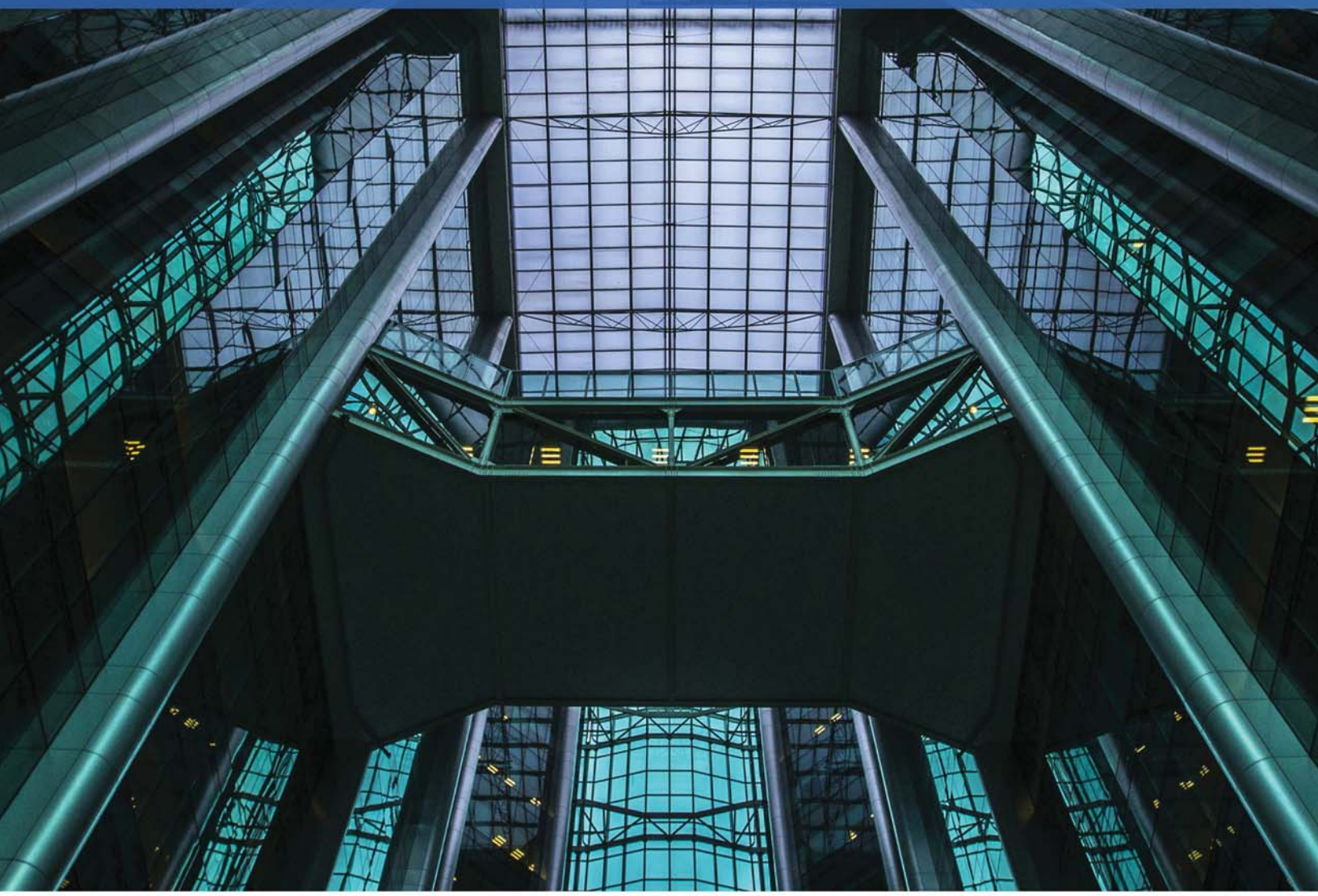
CYBER SECURITY AS A SERVICE:

Opportunities for Financial Institutions, Insurers, and Benefits Providers to Drive Growth and Build Trust



IDT911™

Bloomberg BNA

Cyber Security as a Service:

Opportunities for Financial Institutions, Insurers, And Benefits Providers to Drive Growth and Build Trust

March 2016

Content sponsored by IDT911, LLC

Introduction

The financial services, insurance, and benefits industries face intense pressure to provide customers with services that deliver exceptional value while also building loyalty and trust. They have a long history of developing cost-effective products to protect against risk, but now they must overcome a number of challenges:

- **A hypercompetitive environment** that makes it difficult to recruit and retain employees and customers**.**
- **Nontraditional competitors** encroaching on market share**.**
- **Government regulations** that increase compliance risks.

Changing times demand innovative strategies. One sure way to stay ahead of the competition: partnering with a trusted provider of cyber security services. Financial Institutions, Insurers, and Benefits Providers can keep their data secure with an identity and data defense services partner that works as an extension of their brand to drive growth and enhance employee and customer loyalty.

Data Security As a Competitive Differentiator

Relentless cyber attacks on corporate and consumer data have created a new era of cyber anxiety. Security incidents continue to grow in severity and frequency, experiencing a 38 percent jump in 2015 alone, compared with the year before.[1] Attacks can strike organizations and their employees and customers, compromising these hard-earned relationships.

While businesses are making significant investments to secure their systems and data, individuals are searching for ways to protect themselves against identity theft.

Mounting cyber threats present Financial Institutions, Insurers, and Benefits Providers with a unique opportunity to offer identity and data protection services to their employees and customers as an added value and competitive differentiator. In fact, consumers have come to expect it from their vendor of choice and are increasingly broadcasting their experiences on social media. Most hold businesses and organizations accountable after a breach.[2] Failure to deliver that protection can weaken customer or employee relationships and lead to churn, with one in five victims avoiding business interactions with breached organizations.[3]

---

[1] "Turnaround and Transformation in Cyber Security: Key Findings from the Global State of Information Security Survey 2016," 2, PwC.

[2] "The Consumer Data Insecurity Report," 8, Javelin Strategy & Research, June 2014.

[3] Ibid.

Companies are increasingly turning to cyber insurance as a resource to guard against risk. Cyber and privacy breach coverages can help defray expenses related to services and systems, as well as consumer data, in the wake of an event. But a truly comprehensive cyber security solution will include education, protection and restoration. End-to-end protection will guard a business and its customers at the outset and include:

- Assessing the scope, scale and severity of the breach
- Implementing identity and credit monitoring programs
- Complying with notification regulations, and
- Conferring with a number of parties, including legal teams and regulatory bodies with a regimented vendor selection process.

> "There were a number of different programs that were offered (by IDT911) that we didn't see in the competition (and) because of (IDT911's) pricing structure, we're actually able to bring in revenue."
>
> *—Manny Padilla, VP of Marketing & Business Development, Los Angeles Police Federal Credit Union*

Providers must find ways to distinguish themselves in a crowded marketplace. New entrants, such as credit card companies and credit bureaus, offer a range of products that only deliver selective identity defense services.

Building a comprehensive cyber security program from scratch can be a costly and time-consuming endeavor. To save money and strengthen defenses now, many companies hire outside firms that specialize in identity and data protection, as well as security risk and infrastructure management.[4] This foresight often pays off, since the patchwork of regulations and restrictions governing data security can seem overwhelming.

Regulations, Standards and Other Pressures

The steady surge in data breaches has drawn scrutiny from state and federal government regulators. Mandatory data breach notification laws exist in 47 states (as well as Washington, D.C., Guam, Puerto Rico, and the U.S. Virgin Islands). And there are a number of efforts at the federal level to establish a nationwide notification law. In 2015 alone, Congress considered four bills that would create a federal standard for information security, but there remain some challenges over whether a federal law should supersede state laws.

While cyber security coverage isn't mandatory for businesses, it's clear that regulators are favoring increased protection.[5] And recent initiatives suggest that government oversight will likely increase as cyber attacks proliferate. These developments signal a need for all those involved with consumer and

[4] "Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware," Gartner, Aug. 22, 2014.

[5] "Regulators to Step Up Cyber Security Activity: Lawsky," *American Banker*, July 28, 2015.

employee data to prepare for increased regulatory requirements that could come down the line in the near future.

Financial Institutions

Financial Institutions, in particular, face increased pressure from regulators to enhance cyber security preparedness and protection. And for good reason: The industry is one of the most targeted. According to PwC, 45 percent of Financial Institutions were impacted by economic crime in 2014, compared with only 34 percent across all other industries.[6] Additionally, the industry has the second highest remediation cost, at $170 per record.[7] Recent regulatory initiatives include:

- Security Exchange Commission's 2016 examination priorities
- Federal Financial Institutions Examination Council's push for industry participation in the Financial Services Information Sharing and Analysis Center
- Office of the Comptroller of the Currency's bank supervision operating plan for 2016.

These plans not only prioritize cyber security, they aim to ensure that banks have the proper processes and safeguards in place to protect business and individual customer data. To remain in compliance, financial service providers not only must ensure that their own internal procedures and safeguards are in place, but also that their customers are prepared for a breach and will have access to proven remediation assistance. Studies show that this is good business: 79 percent of survey respondents say they are very likely to do business with an organization because it offers identity monitoring.[8]

Insurance Carriers

Growth in the cyber insurance market has skyrocketed and will reach an expected $5 billion in annual premiums by 2018.[9] But questions remain about the adequacy of these policies. Coverage alone isn't enough for policyholders, according to Paul Delbridge, an insurance partner at PwC. "Given the high costs of coverage, the limits imposed, the tight terms and conditions, and the restrictions on whether policyholders can make a claim, many policyholders are questioning whether their policies are delivering real value," Delbridge said in a 2015 report.

Insurers will miss the market opportunity that cyber security presents if they continue to focus on blanket policy restrictions and conservative pricing strategies. Innovation is required. This can be done through partnering with identity theft and breach management firms that can provide holistic solutions encompassing the entire breach and resulting individual fraud remediation lifecycle. Such a partnership can bolster policy value by offering financial protection, risk mitigation, and streamlined expert breach response strategies.

---

[6] "Threats to the Financial Services Sector," PwC.
[7] "2015 Cost of a Data Breach Cost: Global Analysis," Ponemon Institute.
[8] GfK Omnibus Service Research, May 16-18, 2014.
[9] "Insurance 2020: Reaping the dividends of cyber resilience," PwC, 2015.

Additionally, the National Association of Insurance Commissioners (NAIC) continues to put pressure on Insurers with its Principles for Effective Cyber security Insurance Regulatory Guidance, which directs Insurers, producers and other regulated entities to join forces in identifying risks and adopting practical solutions to protect the information entrusted to them. A component within the guidance calls for planning for incident response by Insurers and other regulated entities, as well as the regulators themselves. Furthermore, NAIC's Roadmap for Cyber Security Consumer Protections, formerly known as the Consumer Cyber Security Bill of Rights, details what consumers can expect from insurance companies, agents and other businesses following a breach.

Employee Benefits Providers

The tide has shifted within the health and benefits industry, predominantly brought on by the Affordable Care Act—in particular, the ACA's virtual marketplaces, mandates for the electronic storage and sharing of patient data, and the steady drive toward self-service. Health care professionals and patients alike are concerned that these changes around sensitive data will attract malicious hackers.[10] Meanwhile, massive data breaches at major national insurance carriers have renewed questions about the security of ACA exchanges.[11]

In addition, the ACA has placed both employees and their employers in the forefront of purchasing decisions. Employers are expecting more from their Benefits Providers, and that's driving increased competition within the industry. To stand out against their rivals, Benefits Providers are turning to new and innovative offerings, moving beyond basic protection, and focusing on value-based offerings that provide added benefits for employers and their employees alike.

Employers also are making efforts to increase productivity, and a factor impacting employees' productivity is their financial wellness. Employees spend two to three hours per week concerned with or dealing with their personal finances, which can eat into company productivity, costing both the employee and the employer.[12] As a result, an increasing number of employers are involving themselves in their employees' financial wellness through services, tools and educational campaigns.[13]

Successful Benefits Providers are meeting this need by expanding their portfolios to include identity theft protection.[14] Considering nearly 20 percent of employees have been a victim of identity theft, the added value provided by this benefit can drive employee loyalty and retention—always a boon for employers—and help differentiate a benefits provider's portfolio from its competition. [15]

This trend is further driven by changes made by the IRS in late 2015, when it expanded its preferential tax treatment for employer-provided identity theft benefits. Previous guidance allowed for preferential tax treatment for identity protection services, but only following a breach and only for those individuals

---

[10] "Obamacare vs. Patient Data Security," InformationWeek Healthcare, March 13, 2014.
[11] "Anthem Hack Raises Obamacare Concerns," The Hill, Feb. 5, 2015.
[12] "5 Signs of Employee Financial Stress," Benefitspro, Jan. 14, 2015.
[13] "Employers Working to Boost Employee Financial Wellness," Benefitspro, Jan. 8, 2016
[14] "How to Protect Your Business and Employees from Identity Theft Risks," Corporate Wellness Magazine, March 10, 2015.
[15] "Employee Financial Wellness Survey: 2015 Results," PwC, April 2015.

whose information may have been compromised. According to the IRS, the guidance was expanded in response to these types of benefits being offered to individuals with increasing frequency.[16]

End-User Knowledge of Fraud and Breach

Business Clients

Keeping abreast of emerging cyber security trends and ensuring that response plans evolve at a similar pace are big challenges for any business. There is a common misconception that only certain industries and larger companies are at risk for data breaches. In reality, breach incidents are indiscriminate, impacting all industries and businesses of all sizes. Criminals are targeting small and midsize businesses (SMBs), many of which lack the resources and knowledge required to develop and implement adequate security programs.[17] And hackers are looking for different types of data, whether for extortion purposes or simply to cause harm.[18] Businesses that already have established a unique position of trust with their business customers are strategically placed to offer robust cyber security solutions.

A shortage of qualified cyber security professionals, however, has prompted leading businesses to seek outside support for risk management, cyber security program development, and security awareness training. "Unprepared organizations, when notified of a breach by external entities, such as the FBI, are increasingly employing professional security service providers to address security emergencies," said Frank Dickson, network security research director at Frost & Sullivan.

Many companies—even those with breach response plans—are overwhelmed by the multitude of security breaches and their aftermath. The number of companies putting data breach response plans in place has increased in recent years. According to a Ponemon Institute Data Breach Preparedness Study, 81 percent of companies have a plan in place—a 20-point increase over just two years ago.[19] Despite this, many companies struggle to feel confident in their ability to manage a breach. According to the same study, "organizations aren't taking into account the full breadth of procedures that need to be incorporated in the response plan and aren't considering the wide variety of security incidents that can happen."[20] Indeed, only 32 percent of organizations rated their response plan as effective for protecting customers and, similarly, only 32 percent said they understand what needs to be done following a material data breach to prevent negative public opinion.

Part of the reason companies struggle to feel confident in their ability to manage a breach is a lack of internal expertise of resources. Companies can address this issue by partnering with a cyber security consultant that can take into account the company's ability to thoroughly implement a plan and make recommendations to improve the company's overall security posture.

---

[16] "Regulatory Clarity Makes ID Protection a More Attractive Employee Benefit," Employee Benefit Adviser, Jan. 20, 2016.
[17] "Cyber Attacks on the Rise: Are Private Companies Doing Enough to Protect Themselves?" PwC, 2014.
[18] "2016 Data Breach Industry Forecast," Experian and Ponemon Institute.
[19] "Third Annual Study: Is Your Company Ready for a Big Data Breach," 2, Ponemon Institute, October 2015.
[20] Ibid.

Employees, too, can play a critical role for businesses in their cyber security preparedness. They are often at the root of cyber breach incidents, accounting for 25 percent of all data breaches—second behind malicious or criminal attacks. The reason? Human error and lack of knowledge relating to proper procedures and security measures.[21] According to the Ponemon Institute, while more companies are putting employee privacy and data protection awareness programs in place, they are often not making them available to employees on a regular basis. Many companies said they offer training only once or sporadically. Similarly, nearly half of companies surveyed said the content of their awareness programs goes without review on a regular basis, and just about half said these programs are not provided as part of new employee orientation programs.

Beyond human error, companies are also at risk due to malicious employees. A malicious insider can be a current or former employee, a contractor, or even a business partner—essentially, anyone with a grudge who has access to a company's confidential personal or corporate information. An Infosecurity Europe study alarmingly found that 37 percent of respondents said they would consider turning over corporate data if it was of benefit to them.

Turning to a partner with IT, privacy, legal and third-party auditing experience can help businesses keep employees engaged, stay up to speed on evolving risk assessments, and, ultimately, minimize overall data-related risk.

Individual Customers

The need for personal cyber security is growing, too, as data breaches that lead to identity theft proliferate. However, many people don't look for identity protection until after they've fallen victim to this fast-growing crime. Identity theft claimed more than 13 million victims in 2015.[22] The crime takes many forms and hits people at every stage of life, but to grasp the severity of this crime, consider the costs: Total fraud losses reached $15 billion in 2015. And in the past six years, fraudsters have stolen $112 billion, or $35,000 per minute.[23]

Resolving identity theft on your own, however, can be an onerous experience. Victims face time-consuming exchanges with many different parties, including government agencies, law enforcement and credit bureaus. It's a lot of red tape.

Many victims who don't know where to go for reliable assistance turn to lawyers or advertised services that are costly or unproven. They're under significant emotional stress and are expecting:

- Unlimited resolution support
- Credit and fraud monitoring
- Document replacement services
- 24/7 support
- Family coverage.

[21] "2015 Cost of a Data Breach Study: Global Analysis," 11, Ponemon Institute, May 2015.
[22] "2016 Identity Fraud: Fraud Hits an Inflection Point," Javelin Strategy & Research.
[23] Ibid.

Costs for these services vary widely, with little guarantee of delivery. Left to their own devices and often acting in response to a notice that they're victims of a third-party breach, customers and employees need a trusted partner that already has been fully vetted.

Selecting the Right Partner

Choosing the right partner for an identity and data defense program is no easy task. Companies must go beyond due diligence to select a partner that is credible and familiar with their respective industry—particularly its government regulation requirements. A partner also should offer a breadth of products and services that address a wide range of client, customer and employee protection needs.

Be wary of data protection services that are one-size-fits-all, as needs will differ from one individual or business to the next. Products and services must be customizable to truly be effective. For example, IDT911's LifeStages® Identity Management Services solution offers on-demand, personalized protection for people of various ages and stages of life, each of which brings its own unique risks.

Equally paramount is a partner's ability to stay abreast of developments in the cyber security space, and to modify its products and services as the identity theft and data breach threats evolve and customer expectations mature.

From an internal standpoint, it's important that such programs are understood by staff in order to be effective. When choosing the right partner, be sure to evaluate their education and rollout capabilities, including program or product development support, program implementation support, program marketing support and flexible training options. The partnership should allow for frequent check-ins to ensure both parties are aware of changes that could impact the need for certain features.

What to Look for in a Partner

- Credibility within your industry
- Customizable and evolving products and services
- Consistent internal support through structured rollout programs, staff education, marketing tools, and regular check-ins
- Superior customer service—and a track record to prove it
- Knowledge of your organization's needs, and the needs of your employees and customers

A trusted identity and data defense partner will act as a true extension of your business. Customers should have access to continuous monitoring of public and private databases, social media channels, and the Internet black market for the presence and possible misuse of customer identities and credit data. Customers also should have access to a team of experienced award-winning fraud specialists and investigators with 10-plus years of experience in the field for preventive and resolution support 24/7.

Conclusion

Identity fraud and data breaches are happening every day and increasing in frequency, severity and impact. They are also continuously evolving with new approaches. By turning to a cyber security partner,

businesses can stay ahead of threats—and the competition—with programs that foster growth and customer and employee loyalty, while remaining in compliance.