Data Protection and Compliance Considerations for Solution Providers

REVEALING REGULATIONS ON SECURITY IN VERTICAL MARKETS

TechTarget Custom Media
A TECHTARGET WHITE PAPER

The more cybersecurity risks continue to grow into board room issues, the more obvious it has become that security offerings are becoming a huge competitive differentiator for savvy IT solution providers. As resellers have been forced by market conditions into becoming true solution and managed service providers, they've needed to change their business models. Instead of focusing on speeds and feeds, functions and features, solution providers now must center discussions around how their portfolio of technologies can truly address business needs and problems, with security fast developing into a top requirement across the chain of command.

In particular, an increased emphasis by solution providers on data protection will help executives with the most top-of-mind security concern today: regulatory compliance. As things stand, most customer organizations are struggling to rein in risks to their data. Data breaches are at an all-time high. Last year alone, more than 1.1 billion personal and sensitive records were exposed across 3,014 incidents, a 22% increase over 2013.[1] As organizations of all sizes have struggled to keep up with increased security risks, regulatory demands from the government and industry have stepped up the pressure on these businesses to start better protecting consumer data. Regulatory bodies are becoming stricter than ever in enforcing fines and repercussions for organizations that don't comply with cybersecurity regulations.

While many veteran VARs that have been in the IT game for a long time have been successful selling software and hardware without making security a primary consideration, it's time for that to change. Successful solution providers will find that going forward they'll need to be a part of the answer and not the problem. This starts with being cognizant of how well current offerings meet compliance and security needs. For example, is a data storage infrastructure stack going to meet auditors' demands?

But the opportunities also extend outward. The best potential is in also building out further products and services to help clients meet their compliance objectives. In order to do that, solution providers first need to understand the lay of the land within the verticals that they focus on.

Here's a cheat sheet for understanding the regulations for four of the vertical markets VARs are most likely to sell into, as well as the data at risk in each market and the costs of a breach.

[1] "2014 Year-End Data Breach QuickView Report," Risk Based Security, February 2015

Retail

The Regulations in Play

The Payment Card Industry Data Security Standards (PCI DSS)–the comprehensive framework of cybersecurity standards required of retail organizations by credit card companies–has become the benchmark for the bottom floor of security controls necessary to protect sensitive customer data. Spread across 12 main control categories, PCI DSS encompasses 255 specific requirements for retail, including logging, monitoring and restricting access to systems containing cardholder data, as well as encrypting sensitive data at rest and in transit. The PCI Security Council entrusted by the payment card brands to maintain the PCI DSS standard works with the retail industry and other players in the payment card ecosystem to constantly update these standards to keep up with threat trends and advances in technology. For example, one of the latest requirements pushed by payment brands and the standards is the use of EMV chips to encrypt payment data at the point of sale and add additional authentication in the transaction to prevent card fraud.

Experts with Verizon's PCI Consulting Services group recently told the National Retail Federation that, while there's been an 80% increase in PCI compliance within retail organizations, only 29% of organizations are able to maintain PCI compliance on an ongoing basis.[2]

The Data at Risk

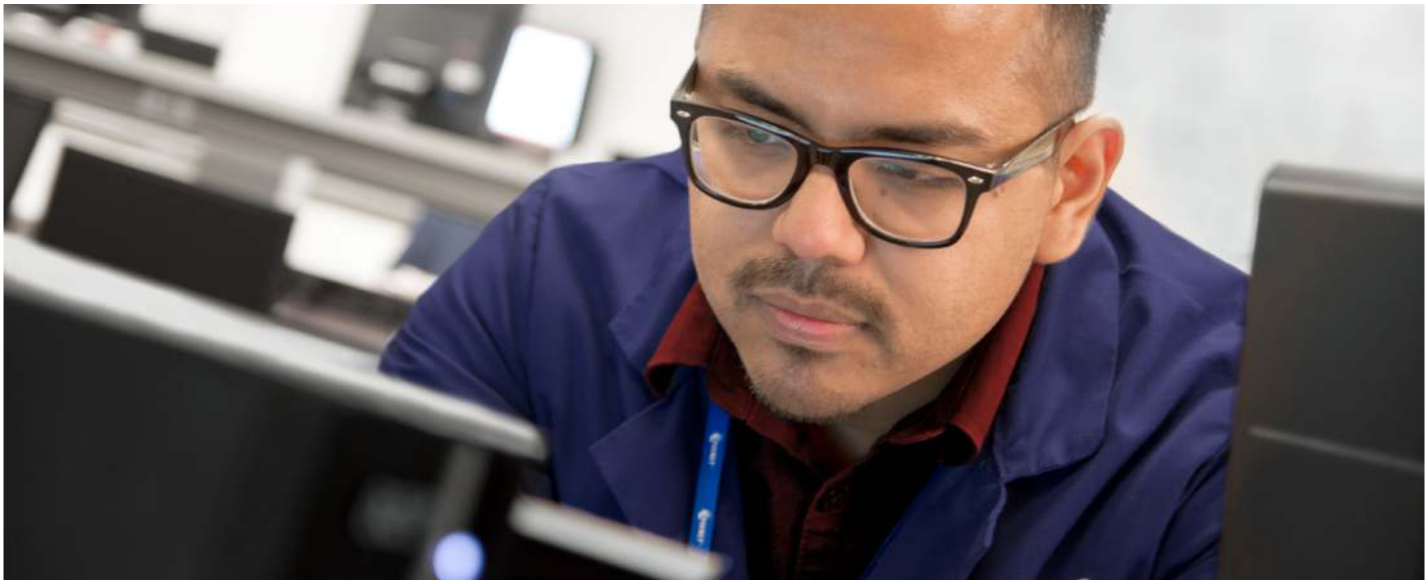
Retail organizations must protect a host of regulated and sensitive data collected and transmitted across their IT systems. The most prevalent data includes cardholder and personal data as governed by PCI standards. And increasingly, as retailers move to online and mobile-friendly transactions, Web history and location data also comes into play.

Breach Costs

Average cost per personal record breached: $165[3]

[2] "Strength Training," National Retail Federation, June 4, 2015

[3] "2015 Cost of Data Breach Study," Ponemon Institute, May 2015



Energy/Utilities

The Regulations in Play

As a part of our nation’s critical infrastructure, it’s understandable that energy and utility companies would fall under a number of different regulatory frameworks. VARs that cater to energy-related companies should be mindful of three major energy compliance acronyms as they navigate the regulatory jumble in this industry vertical: NERC, FERC and CIP. The North American Electric Reliability Corporation (NERC) is sanctioned by the Federal Energy Regulatory Commission (FERC) as the main body responsible for maintaining the electric reliability for the U.S. In order to carry this out on the cyber front, NERC developed what is called the Critical Infrastructure Protection (CIP) standards, which are the main cybersecurity reliability standards for the energy industry.

The Data at Risk

At the most obvious level, energy and utility companies are entrusted with a host of customer information needed to service and bill their customers on a month-by-month basis. This includes payment information, bank records and contact information. But as utilities ramp up their use of smart grid technologies, the kind of data they collect on customers becomes increasingly sensitive. Smart meters collect data about customer usage patterns and status, which criminals could potentially use to create profiles on customers.

> From a public safety perspective, even more concerning is the kind of infrastructure information that could put energy grid reliability and security at risk should it be breached. Whether it is information about the power plants themselves, substation information such as transformer or line status, or pipeline status data, this information is of the utmost sensitivity and is typically governed by the regulations named above.

Breach Costs

Average cost per record: $132[4]

[4] “2015 Cost of Data Breach Study,” Ponemon Institute, May 2015

Financial

The Regulations in Play

With so much money at stake and a target firmly on their backs for cybercriminals and fraudsters to take aim at, financial institutions contend with some of the most challenging cybersecurity concerns. In addition to being subject to all of the same PCI considerations as retail organizations–financial institutions, after all, deal in credit cards–there are many others that solution providers need to educate themselves on in order to fully understand this vertical and meet institutions' security and compliance needs.

For example, the requirements of the Sarbanes-Oxley Act (SOX) drive larger organizations to enact strict access controls and enforce segregation of duties so that employees can only access information appropriate for their role in the organization. The act also requires stringent monitoring and reporting to provide a documented trail of evidence for auditors.

Meanwhile, though the Gramm-Leach-Bliley-Act of 1999 primarily has to do with broad-based banking practices, it includes provisions that require banking institutions to protect their networks and the integrity of the data that runs today's modern banking infrastructure. Additionally, federal agencies like the FDIC, SEC, FFIEC and FINRA all have their own overlapping laundry list of requirements to protect consumers and the integrity of digital banking.

The Data at Risk

Banks collect and hold the most sensitive consumer data, information that controls people's financial freedom and well-being. In addition to personally identifiable information, account information and details about customers' financial holdings they're trusted to protect, these institutions also need to worry about the trust in their brand that comes from protecting the integrity of IT data operations. Without appropriate protections in place, attackers or insiders could manipulate systems for fraudulent purposes–not only defrauding the institution, but also potentially doing irrevocable damage to that bank's reputation as a trusted institution.

Breach Costs

Average cost per record: $215[5]

[5] "2015 Cost of Data Breach Study," Ponemon Institute, May 2015

Healthcare

The Regulations in Play

Currently, about 11% to 12% of healthcare IT is dedicated to information security, according to a recent HIMSS study.[6] The Health Insurance Portability and Accountability Act (HIPAA) was another broad-brush law that included a number of privacy rules, among them those governing the safety of patient information in digital format. For many years, HIPAA was a law without much bite to it, as many healthcare organizations let their cybersecurity practices languish, assuming there was little enforcement of HIPAA rules.

The Health Information Technology for Economic and Clinical Health (HITECH) Act changed the game in 2009 by not only adding teeth to HIPAA enforcement, but also adding requirements for healthcare organizations to further digitize their operations through adoption of electronic health records (EHR) in order to receive the maximum levels of Medicare/Medicaid funding. In the same HIMSS study, 51% of respondents indicated that their organization has increased the budget and resources dedicated to information security as a result of federal initiatives impacting privacy and security such as audits by the Office for Civil Rights (OCR), Meaningful Use and the HIPAA Omnibus Rule.

In addition, providers must institute Meaningful Use into their EHR technology. This is a double whammy for healthcare institutions. On one hand the pressure is high to reduce the security risk to existing digital assets, while on the other hand they are being forced to provide electronically stored patient information to their patients/surrogates, physicians' other healthcare organizations, health information exchanges, payers and state, local and federal agencies.

Additionally, that pressure is only growing as the volume of data entrusted to IT increases through the meaningful use of EHR systems. In addition to these specialized compliance concerns, healthcare is also largely under the domain of PCI compliance, as most healthcare institutions process credit cards in large volumes.

[6] "6th Annual HIMSS Security Survey," HIMSS, February 19, 2014

In some instances, the US government can levy fines of up to $1.5 million for severe security lapses.[7] The government also mandates inclusion on the U.S. Health and Human Services "Wall of Shame," which has grown rapidly over the past few years.

The Data at Risk

Healthcare organizations are responsible for keeping protected health information (PHI) and cardholder data safe.

Breach Costs

Average cost per record: $363[8]

91% increase in cyberattacks in 2013[9]

$34 million records stolen since 2009[10]

$1.6 billion costs associated with healthcare breaches[11]

[7] "6th Annual HIMSS Security Survey," HIMSS, February 19, 2014

[8] "2015 Cost of Data Breach Study," Ponemon Institute

[9, 10, 11] "6th Annual HIMSS Security Survey," HIMSS, February 19, 2014

Drowning in Threats

The Regulations in Play

According to the Trustwave Security Pressures report, only 16% of organizations today believe they have the ideal staffing and skills level to appropriately handle security incidents as they come up.[12] Many organizations today are drowning in cybersecurity threats and even if they invest in security software or hardware, they may not have the skills or expertise to analyze threats and respond to incidents in a timely fashion to prevent attackers from absconding with their data. Solution providers are in a great position to help their clients by offering up services and skills to manage security functions that these organizations would otherwise be unable to provide in-house.

It's why analysts with Allied Market Research estimate that the managed security services market will grow 15.8% year-over-year through 2020 to eventually reach $29.9 billion by the end of the decade.[13]

For organizations that have never made security solutions a primary focus, now is the time to think about how data protection plays into their business model. Here are some suggestions on where to start:

- Ask, "Why are you buying this?" For traditional infrastructure VARs, every time they sell storage or servers, they should be asking the customer if they will be encrypting the data stored on that hardware. This is low-hanging fruit for an easy upsell.

- Know the customer's calendar. With the holiday season approaching, solution providers have a tremendous opportunity to offer security assessment services to customers to ensure websites are penetration-tested or data is secure before the heavy load of the fourth quarter approaches.

- Many solution providers are considering a move to consumption-based services sold in the cloud, but security is a huge gap for cloud today and there are a number of offerings on the market that can solve that problem for customers moving workloads to the cloud.

Adding Value With Defense in Depth

No matter what vertical solution providers sell into, they should remember that their clients' executives increasingly view compliance and security of products and services as a non-negotiable evaluation metric. Solution providers need to understand how well their solutions meet compliance standards. The more solution providers invest in embedding security into their sales model, the more benefits they'll reap. Though many customers do view security as table stakes to some degree, there will be better results for those solution providers that go above and beyond by providing security tools in their products and services that aid customers in their compliance journey.

Additionally, solution providers stand to improve their business by considering building out a portfolio of security products that move beyond the standard moat-and-castle approach of perimeter security technologies. This means helping clients invest in technologies and services that help with the following:

Control	Technology
Control and monitor access to data	Identity and access management, network access control
Detect exfiltration of data	Data leak prevention
Obfuscate data on the chance that data stores are broken into	Encryption, tokenization
Protect the most sensitive data stores	Database security

[12] "2015 Security Pressures Report," Trustwave, 2015

[13] "Global Managed Security Services Market (Deployment Modes, Organization Size, Applications, Verticals and Geographies) - Size, Share, Global Trends, Company Profiles, Demand, Insights, Analysis, Research, Reports, Opportunities, Segmentation, Forecast 2013 – 2020," Allied Market Research, April 2015

Technology Security

Working With Avnet Technology Solutions

With our technology expertise, strategic alliances, training, resources and services, we provide complete customer solutions that span the data center and IT lifecycle. Working with Avnet, you will:

- Speed time to market
- Increase sales and profits
- Minimize investment and risk

Avnet Technology Solutions connects solution providers to the leading-edge technology, resources and expertise they need to provide comprehensive security solutions that account for everything from unique workflow requirements to industry regulations for privacy and data-loss prevention.

Are you ready to explore the benefits of better cyber-security? Start here.

As a global IT solutions distributor, Avnet Technology Solutions transforms technology into business solutions for customers around the world. It collaborates with customers and suppliers to create and deliver services, software and hardware solutions that address the changing needs of end-user customers. The group serves customers and suppliers in North America, Latin America and Caribbean, Asia Pacific, and Europe, Middle East and Africa. It generated US $10.6 billion in annual revenue for fiscal year 2015. Avnet Technology Solutions is an operating group of Avnet, Inc. For more information, visit http://www.ats.avnet.com.

Avnet Technology Solutions
1-800-409-1483
8700 South Price Road
Tempe, AZ 85284
www.ats.avnet.com