SECURITY AND COMPLIANCE: TWIN CHALLENGES CALL FOR UNIFIED RESPONSE

Today, business is digital. Data of all kinds is speeding across worldwide networks to and from data centers and cloud services, even as data quantities steadily increase, fueled by low-cost storage and a burgeoning array of Internet-of-Things (IoT) devices. But as digital business opportunities expand, companies face a number of daunting challenges. Foremost among them is the growing number of cyber attacks, as threat actors proliferate across a variety of attack vectors. In addition, the interdependence of business and data has spawned new regulatory guidelines that span industries and geographic regions. To survive and thrive, businesses must meet the twin challenges of security and compliance.

SECURITY CHALLENGES: THREAT ACTORS

Today's security threats come from a wide array of perpetrators who are responsible for ever-more dangerous attacks.

NATION-STATES: Perhaps the most capable and therefore the most difficult to defend against, nation-state-backed threat actors' goals are espionage and disruption, supported by the resources and protection of a government. Compounding the challenge, rogue information brokers such as WikiLeaks have made toolkits developed by nation-states available to many others.

CYBERCRIMINALS: To achieve financial gain, cybercriminals' traditional aim is to steal credit card numbers. Personal health information (PHI), is also a recurrent target, with the goal of perpetrating

insurance fraud. However, the advent of ransomware, such as the huge WannaCry ransomware hit that happened all over the world in early May, has opened up a new front. Phishing attacks and accompanying ransom demands have brought cybercriminals millions of dollars in ransom payments. Many victims have decided it is faster and cheaper to pay the ransom rather than resist.

HACKTIVISTS: With the goal of disruption to right, or draw attention to a perceived source of social injustice, hacktivists, many under the Anonymous umbrella, launch denial-of-service attacks or steal and disclose information. While not as prevalent as in previous years, hacktivists remain a threat.

TERRORISTS: While generally lacking the sophistication of other threat actors, terrorists' goals are to spread fear and encourage unrest. The risk is present and growing.

INSIDERS: Employees, contractors, and third parties with knowledge of a company's data and systems wreak a considerable amount of havoc, driven by the motivations of revenge or greed.

Today's security threats come from a wide array of perpetrators who are responsible for ever-more dangerous attacks.

ATTACK VECTORS

Businesses are the targets of attacks from many directions, both traditional and new.

EMAIL: Phishing attacks through email continue to be highly effective. By using malicious attachments and URLs, actors trick victims into clicks that trigger compromise. These attacks are difficult to defend against because email is used for such a large amount of business purposes and the sheer quantity of phishing attempts leads to the likelihood of one of them succeeding through a negligent employee. In recent spearphishing attacks, actors have posed as corporate officials, requesting and obtaining the W-2 information of all employees, enabling tax refund fraud and identity theft.

WEB BROWSERS: Web browsers have been a prevalent interface for business users for over two decades. Browsers must be updated regularly in order to protect against the latest threats. Plug-ins also must be updated frequently with versions containing the latest security fixes. Out-of-date browsers and plug-ins are targets that never go out of style for attackers.

INTERNET OF THINGS: The IoT has attracted much attention because of its potentially game-changing benefits to businesses. But many organizations are leaping into IoT without taking into consideration risks from the software that runs the IoT devices. In many cases, that code, or significant components in the build is not written by the IoT vendor and may be of dubious quality. IoT devices are not always architected with security in mind and they may not be patchable and upgradable. The result is a proliferation of security vulnerabilities across a myriad of devices.

CLOUD AND MOBILE: Although their use is widespread, the fact that both may be chosen by end users without the involvement of IT introduces risk and limits an organization's ability to

manage that risk. For example, a user may employ his or her own BYOD smartphone and perform an unauthorized upload or download of files from a cloud-based collaboration service. This behavior is hard for IT to prohibit, and could expose an organization to threats without IT being aware. In addition, smart phones, laptops, tablets, and USB devices all can store large amounts of data, which can fall into the wrong hands should a device be lost or stolen.

SECURITY AND COMPLIANCE

Despite the broad array of threat actors and attack vectors, businesses must keep data secure but also available. To this end, a number of organizations have established security standards geared to the needs of different industries. Compliance may be voluntary or mandatory, and compliance certification may carry legal obligations. It's important to understand that the compliance programs identify the minimum level of security required, which may not be adequate to address the next generation or even the current threat landscape.

PCI Security Standards Council—The council is a global forum for developing, enhancing, and implementing security standards for the protection of sensitive payment card information. Compliance with PCI Security Standards engenders trust among merchants and payment card users.

NIST Cybersecurity Framework—The U.S. Department of Commerce's voluntary guidelines help organizations understand, manage, and reduce cybersecurity risks. The framework gives companies, particularly buyers and suppliers, a common way to communicate their cybersecurity readiness.

Privacy Shield—The framework for transferring personal data securely from the European Union and Switzerland to the U. S. is essential for compliance with European privacy regulations. While participating in Privacy Shield is voluntary, once an organization commits publicly to compliance, the commitment becomes enforceable under U. S. law.

HIPAA Security Rule—This requires health care industry participants to protect the privacy of electronic personal health information (PHI). Health care organizations must ensure the confidentiality, integrity, and availability of electronic PHI, safeguarding it against reasonably anticipated threats and impermissible disclosures.

Health Information Trust (HITRUST) Alliance—This privately held company has established a Common Security Framework (CSF) for organizations that create, handle or store sensitive health care data. The standards derive from NIST, PCI, HIPAA and ISO.

SOC 1 and SOC 2—From the American Institute of Certified Public Accountants, Service Organization Control (SOC) 1 sets forth standards for internal controls over financial reporting. SOC 2 applies to data centers, IT managed services, and cloud services. It covers security, availability, processing integrity, confidentiality of information, and information privacy.

COMPLIANCE

Businesses are expected to know and follow the guidelines that pertain to their industry. In many industries, the standards for protecting data are considered mature, and as a result, enforcement

is increasingly stringent and punishment severe. For example, in December 2015, the U.S. Federal Trade Commission levied a $100 million fine against LifeLock for violating an earlier court order requiring it to secure consumers' personal information and prohibiting the company from deceptive advertising. The company had falsely claimed that it protected consumers' data with the same high-level safeguards used by financial institutions.

In 2016, a fine of $5.55 million was levied by the Department of Health and Human Services against Advocate Health Care of Downers Grove, Ill., the largest HIPAA fine against a single entity. The fine was due to breaches that compromised the electronic PHI of 4 million individuals, including their names, demographic information, addresses, credit card numbers, dates of birth, clinical information, and health insurance information. The breaches took place as a result of the theft of an unencrypted laptop computer from an unlocked vehicle.

Despite such troubling precedents, many organizations view compliance as an expense to be borne and therefore do the minimum required. Some companies erroneously consider security more urgent and important than compliance. In fact, the two must be addressed together.

Rather than using spreadsheets to manage different compliance initiatives, a Governance, Risk, and Compliance (GRC) tool may provide a unified compliance framework that can help automate compliance documentation.

Companies should start by taking stock of their level of compliance. The goal should be to prepare for an audit, either for self-certification or certification by an outside body. Organizations with a strong compliance foundation are better positioned to build out their security programs. The audit is the key feedback tool to determine a company's level of compliance. Audit readiness is a key discipline for organization to develop, not only to be prepared for an audit but to perform the audit economically and to avoid audit fatigue in the organization. Audit readiness consists of four key steps:

+ Scope—Auditees should clearly understand the system boundaries, processes, and time period of the audit—for example, a point in time vs period of time assessment.

+ Evidence of Controls—Auditors test controls via inquiry, observation, review of evidence, and/or re-performance. Auditees should determine in advance the type and amount of evidence to retain for the execution of each control.

+ Information Repository—Auditors utilize standard transaction population queries, such as new hire listings and change request listings, to perform sampling. Standardizing and centralizing the collection of this information can dramatically increase audit efficiency and reduce audit fatigue.

+ Communication—Establishing timely reporting procedures for audit findings that don't wait for the final report will allow organization to remediate findings and fix potential security holes more quickly, before the findings are reported.

AUDIT ABCs

A UNIFIED SECURITY AND COMPLIANCE RESPONSE

While both security and compliance are of critical importance, companies must satisfy the needs of both in an economical manner. Allowing costs to balloon out of control can imperil a company's survival just as easily as a massive security breach or hefty regulatory fine. As a best practice, the watchwords should be harmonization, integration, and separation.

+ Harmonization—harmonize where compliance standards overlap and identify where the same controls can satisfy multiple compliance requirements.

+ Integration—Implement a strategy that integrates the controls needed for different standards. Doing so will keep costs low.

+ Separation—Separate out systems that require unique compliance controls, so that the additional cost of these controls are isolated to those systems

Rather than using spreadsheets to manage different compliance initiatives, a Governance, Risk, and Compliance (GRC) tool may provide a unified compliance framework that can help automate compliance documentation. GRC platforms can work together with asset management applications, vulnerability scanners, incident response systems, risk management, and audit applications to provide an integrated approach to your security and compliance program.

QTS SOLUTIONS

QTS delivers solutions to provide both security and compliance so businesses can meet the requirements of standards audits.

SECURITY

QTS takes a multi-layered approach to security, encompassing the physical building as well as cyber security.

+ **Physical security** covers property setback, fencing, active guard patrols, ID checks, visitor screening, active video monitoring, and biometric access control. The result is 24x7x365 security from property perimeter to the data center door

+ **Cyber security** is built into all QTS managed offerings. In addition, the QTS Managed Security Suite incorporates seven layers of defense to address specific needs including data encryption, IDS/IPS, firewalls, strong authentication, and VPN.

COMPLIANCE

A dedicated internal audit team helps businesses define controls and processes to meet compliance requirements, with an eye toward adapting to regulations as they change in the future. QTS professionals are expert in a number of compliance standards, particularly those covering the financial services and health care industries.

+ **PCI DSS.** QTS data centers, managed hosting facilities, and cloud services are certified for compliance with PCI DSS.

+ **HIPAA.** QTS healthcare solutions streamline IT operations, lower costs, and above all, protect patient data. QTS platforms comply with HIPAA and HITECH standards.

THE RIGHT PARTNER

Both security and compliance are disciplines in which experience can pay significant dividends. Awareness of the various threat actors and the latest attack vectors is a specialty requiring unceasing focus. Similarly, knowledge of industry security frameworks, enforcement penalties, and audit methodologies requires ongoing dedication. In addition, continuous monitoring for compliance is a best practice in many industries. Because it is often difficult for companies to hire and retain an in-house team with the required expertise in all these areas, a skilled and knowledgeable partner can fill an important need.

Managing security, compliance, and the audit process across a hybrid cloud environment also requires special expertise. Cloud service providers bear some of the responsibility for security and compliance and it is important for customers to understand when they or the cloud provider are responsible. The same is true for third-parties that provide data center services. This is often times called a shared model of responsibility for security. An experienced partner can provide the objectivity required to assess the level of compliance responsibility of cloud service providers, third parties, and the customer.

Establishing a long-term relationship with a partner that can handle both security and compliance provides many benefits. Although each realm requires different expertise, a partner such as QTS provides a single point of contact and can assure that experts in each area work together.

With an ongoing relationship, lines of communication between the customer and the partner can be established, leading to a high level of responsiveness.

Digital business has wrought many changes. But it's a safe bet that still more changes are in store.

A partner with a broad spectrum of expertise like QTS can provide the guidance that's needed as new security challenges emerge, compliance requirements advance in complexity, and new business models come into being.

REFERENCES

- Privacy Shield
- HIPAA Security Rule
- NIST Cybersecurity framework
- SOC 1 and SOC 2
- PCI Security Standards Council
- HITRUST Alliance
- HIPAA fine against Advocate

CONTRIBUTORS

ABOUT QTS | 877.QTS.DATA | QTSDATACENTERS.COM

QTS Realty Trust, Inc. (NYSE: QTS) is a leading provider of secure, compliant data center, hybrid cloud and managed services. QTS features the nation's only fully integrated technology services platform providing flexible, scalable solutions for the federal government, financial services, healthcare and high tech industries. QTS owns, operates or manages more than 5 million square feet of data center space and supports more than 1,100 customers in North America, Europe and Asia Pacific. In addition, QTS' Critical Facilities Management (CFM) provides increased efficiency and greater performance for third-party data center owners and operators.