Five Things Nearshore Vendors Can Do to Allay Client Security Fears

Ensuring you have a clear policy, creating a security culture, addressing physical issues, showing that you know the terrain and demonstrating engagement with government cyber-security initiatives is key to reassuring your clients that their data is secure.

By Bianca Wright July 30, 2015

Photo by Chris Amelung

The need to ensure data security of client data is a non-negotiable. For more large companies, it isn't a question of if a breach will occur, but rather when it will. In such a context, the need for outsourcers, particularly those in the nearshore, to demonstrate their capacity to keep data safe is paramount.

While some data points to outsourcing of IT as a potential security risk, outsourcers have demonstrated their commitment to protecting their clients' data and intellectual property. Alex Hamilton, CEO of Radiant Law, said: "Security has been a high priority for outsourcing customers

for many years, and the outsourcing providers are now well used to having to demonstrate that they take the protection customer's data very seriously."

He added that, with an increasingly sophisticated industry that is used to meeting the high standards of banks and other demanding customers, there is no reason to think that outsourcing would weaken security; in fact it is often the case that standards are raised.

As Jon Butler of ISG said: "The best way to handle a security event is to never have one." However, that is not likely in an environment where breaches are an everyday occurrence. "Today security comprises so much more than just locking server rooms and installing desktop anti-virus software. While many clients do a good job using tools like Citrix or VMware to centrally manage data access, local data center security concerns remain, and clients should mitigate these," he added. So how can vendors put their clients' minds to rest?

Ensure There's a Clear Policy

A negotiated policy on data security needs to meet the needs of both the client and the vendor. There may be specific requirements embedded in the policy, depending on the geography, the client and the circumstance.

The outsourced center needs to comply with international security standards, such as BS-7799, ISO-17799, for example. "Independent audit results are the best proof a

center can offer regarding its level of security. Clients should insist their service provider centers meet these international standards," Butler said.

He added that background check policies – responsibility and thoroughness – are another indicator of security adherence. "Are they done by reputable 3rdparty companies and do they encompass all possible areas to legally check? Additionally, center policy should dictate that on-premise security be run by a separate company that regularly reports incidents. Clients should have access to those records," he said.

Transparency and client access are also key to this. A client who knows the specifics of how its data is secured and what is being done in specific situations. Ajay Gupta, Director, Governance, Risk and Compliance, Capgemini emphasized that an outsourced environment requires having effective and scalable technologies, robust processes and knowledgeable resources to empower clients to continuously innovate and focus on the core business without compromising security.

Create a Security Culture

Gupta said that it is important to promote a "security culture" across the organization by providing relevant security awareness trainings to employees, third party contractors and business partners.

This is vital to ensure that security remains compliant with

the negotiated policy and with the legal and regulatory requirements, regardless of who is handling the data.

Tied to this, said Gupta, is ensuring that there are robust and well written processes with controls built-in the work flow and the well-trained employees to follow them to minimize errors and defects.

Part of the security culture involves the need to conduct ongoing security reviews (internal and external) to measure the effectiveness of security policies and mechanisms deployed by the organization. "Assessment results should be shared with various stakeholders like the organization's Internal Auditor, senior management and clients. For example, vendors should share the SOC 1/SOC 2 reports with clients. These reports provide an independent view on the security aspects of the organization," Gupta said.

Address Physical Issues

Whether it is the physical access to an area or issues with the location of the center or outsourcer, it is important to address these potential factors upfront and explicitly.

Butler said: "I don't think there's a data center at which I couldn't find at least one physical violation." These potential physical violations include things such as actively enforced secure bay entry for project personnel, camera monitoring, audited anti-pass back capability, separate secure room cabling (logical and physical), mailroom security, isolated

digital telephones, machine level security (e.g. USB disablement), customs/bonding legal restrictions, etc.

"It's scary how easy it can be to enter areas without proper authorization. I have been able to hurdle past security just by knowing the cultural "hot buttons" and when to hit them – not a good thing!" Butler said.

Common sense dictates that it is not a good idea to locate a center near dangerous, high-activity or potentially volatile areas. "These include obvious things like flood plains and seismic faults, as well as the not-so-obvious: airports, police stations, military bases, government offices, power stations, mass transit stations, etc. It's best to be far away from areas where potentially unhappy people can forcibly enter the center and gain access to client information," Butler said.

If a city or part of a city is known for such potential issues, vendors need to clearly outline how their security addresses those possible security risks. Reputation does not necessarily translate into increased risk, but perception can mean the difference between landing a client and not.

Show That You Know the Terrain

This is what Butler calls Perspicacity. "Clients should discern how shrewd their service provider is regarding its

surroundings and how it mitigates the unknown," he said. Types of questions to ask include:

- Is it wise for people outside the center to know that work for an international financial institution goes on inside?
- When events occur, would center personnel call the police, and are the police trust-worthy?
- Are mainstream news sources credible?
- Have high-priority arrangements been made with fuel providers for backup generator diesel fuel?

"These are all great areas to probe when making unannounced security audit visits – which you absolutely should be allowed to do! Whether there is a pandemic, pandemonium, an attack by the People's Republic of wherever – clients should insist their center practices and plans for these unpredictable events," Butler said.

He added that service providers should be able to demonstrate to their clients that when chaos reigns that they have well-rehearsed plans for each scenario that validate their data security preparedness so that local security events remain non-events for the center.

Demonstrate Engagement with Government Cyber-security Initiatives

According to Alan Berman, President of DRI International, (Disaster Recovery Institute), a business continuity certification and education nonprofit organization, the

Comprehensive National Cybersecurity Initiative presented in May 2009 established a framework for creating a more secure cyber environment. He noted that it sought to establish a set of major objectives; establishing a defense against immediate threats, enhancing the security of supply chain vendors and expanding education, research and creating strategies to deter hostile and malicious activityin cyberspace.

"While the singular efforts being employed to combat the threat of cyber terrorism should be applauded, these alone will not solve the problem," he said. "Simply creating a strong defense with no threat of punishment to cyber-terrorists will not be enough of a deterrent to create an effective barrier to continued attacks. Only an integrated public/private sector sharing of information, in a secure environment, to quickly identify threats and the ability to engage in offensive destruction of perpetrators ability to continue to function will slow the spread of cyber-terrorism."

By demonstrating that vendors are engaging with the various government initiatives in the USA and in nearshore locations, vendors can emphasize their commitment to security and to the eradication of cyber-terrorism.

SHARE

Tags

Analysis | Ajay Gupta | Alex Hamilton | Capgemini | cyber security

cyber terrorism | Data Security | Jon Butler | Online security | Radiant Law

Bianca Wright

NSAM Managing Editor Bianca Wright has been published in a variety of magazines and online publications in the UK, the US and South Africa, including Global Telecoms Business, Office.com, SA Computer Magazine, M-Business, Discovery.com, Business Start-ups, Cosmopolitan and ComputorEdge. She holds a MPhil degree in Journalism from the University of Stellenbosch and a DPhil in Media Studies from Nelson Mandela Metropolitan University.