Update

Sourcing & Vendor Relationships Advisory Service
Executive Update Vol. 11, No. 6

The Debate Surrounding Information Security Outsourcing

by Justin Kim and Dr. Sara Cullen,
Senior Consultant, Cutter Consortium

Outsourcing has become an integral part of nearly every organization. Whether it is a small business handing over its bookkeeping to a local accountant or the US military outsourcing its security to private companies, it's happening every day around the globe. One area that many organizations largely outsource is IT, an issue that is hardly controversial today. Except for one component — information security outsourcing (ISO).

A recent study found that only 13% of organizations outsource some part of information security.[1] Another went into more detail, showing that while 59% outsource attack-and-penetration testing, only 19% do so for forensic and fraud support.[2]

Like any other outsourcing areas, many experts in the field argue for and against ISO. Some say information security should never be outsourced, while others say that using expertise of a security outsourcing supplier makes a great business strategy. Some claim ISO creates complexity, is less secure, and still requires the organization to take all the responsibility. On the other side, those for ISO say that it is more secure and cost-effective.

Studies, surveys, and expert opinions support all of these claims. Some say that more people with access to data increase risk of a data leak, while others say more eyes will catch more errors. Some say that outsourcing suppliers are better at security, yet others suggest inhouse employees are the only ones who can truly know what information is critical. In this *Executive Update*, we look at each side of the debate.

ARGUMENTS AGAINST ISO

Many of those in charge of information security believe that it should be kept inhouse. The core idea behind information security is to prevent other people from accessing information. Thus, outsourcing would defeat the primary purpose of information security. Cesare Tizi, former CIO of Australia's largest energy supplier, AGL Energy, never outsources the security part of IT.[3] He says that he might outsource security auditing, but when it comes to policy making and critical decisions, he has always kept it inhouse. A main reason is due to privacy information about customers; the risk of someone harvesting that information for nefarious use is just too high. Tizi believes that other organizations cannot be entrusted with information *that* critical.

WhiteHat CEO Rosaleen Citron also believes that security should never be outsourced: "No matter whose fault it is, when [a] company's security is breached, customers always blame the company, not the outsourcers."[4] In *InformationWeek*, Robert Weiler, another senior executive, echoes Citron's comment.[5] He claims that ISO providers, in most cases, have a clause in their contract stating that they cannot possibly find every security flaw and that they are not responsible for any security breach. This means that if a company outsourced information security, is attacked, and information is stolen, then the company — not the ISO provider — will be liable for the security breach.

Dean Prevost, president of IT services at Allstream, claims that by allowing an ISO firm access to secure information in an organization, access control is that much more complex.[6] Organizations that are outsourcing information security have to be even more vigilant about who has access to what. Some say that by outsourcing information security, an organization can add risks to their already vulnerable security.[7] Not only does the organization need to worry about its own

employees, but because of outsourcing, it also must worry about ISO suppliers' employees.

ARGUMENTS FOR ISO

Some people in the outsourcing industry suggest that an ISO is a great idea for organizations. Granted, most of them are outsourcing suppliers and are trying to sell their services, but some points they make do hold some valid arguments. For the most part, their claims are related to finances and expertise. The underlining idea is that an outsourcer can do it cheaper and better because that's its core business, and it does so on a large scale. Some go as far as comparing themselves to doctors.

Bruce Schneier, chief security technology officer of BT and blogger for *Schneier on Security*, draws similarities between ISO and healthcare professionals.[8] He uses the analogy that everyone outsources healthcare and thus all should outsource information security. Not many organizations hire a full-time medical staff on standby just in case someone needs medical attention. They "outsource" it to hospitals and other medical facilities when it is needed. It is far more cost-effective to use outside services rather than have a full-time medical staff and a medical department at each organization. Moreover, it is better to trust healthcare services to a hospital, which does nothing but healthcare, rather than have an inhouse medical staff who deals with an emergency once every six months. He says that information security emergencies happen to any organization only a few times a year, so why hire full-time staff who are going to "work" only once or twice a year? To him, security is eight weeks of relaxation followed by eight hours of panic, and then another six weeks of relaxation and four hours of panic. Thus, it's far better to outsource information security because it is cost-effective, and ISO suppliers are much more experienced in handling incidents than inhouse staff.

According to Schneier, hiring a good security expert can also be a major challenge for organizations. Even if one manages to hire a security expert, he claims that the person doesn't keep the job very long. A good security expert is always looking for a challenge. He or she requires consistent demands that can come only from servicing multiple clients and dealing with new threats daily. That can involve learning something new from one client to spread out the cost and knowledge among others. For a security expert to protect just one organization would be like having a doctor take care of just one patient. It is much better for an expert to work for an ISO supplier, and it is better for an organization to hire a well-known outsourcing supplier than try to hire multiple security experts.

An article by Marie Alner also points out several specific benefits of ISO, such as cutting staff to reduce costs.[9] Variable costs can be turned into fixed, monthly costs, making financial planning more suitable. Above all else, like Schneier, Alner claims that hiring an outsourcing supplier is lot more cost-effective than hiring a team of security experts to do the same thing. She points out that maintenance of information security hardware can become very expensive. Often, the infrastructure is stored in various expensive data centers, which provide cooling, power, and redundant Internet connections to keep the network running. All these expenses can be transferred to an outsourcing supplier. Because it is always keeping up with the latest technologies, the supplier has better security standards, technology, and policies about keeping up with new threats. Thus, security is better left with the experts.

IT expert Yogi Shulz says that outsourcing security reduces cost and rarely adds risks.[10] Many worry about risks that come with outsourcing security, but Shulz says that risk coming out of outsourcing is about the same, if not less, than keeping an inhouse staff. Hiring an outsourcing supplier is actually safer than hiring an employee. While an ISO supplier's reputation can be checked from other organizations, an inhouse employee's history can be kept in the dark. Studies also show that more than 80% of security breaches happen internally and not by external hackers.[11] ISO suppliers are more likely to catch internal errors than inhouse staff. Risk of staff turnover exists in both inhouse and outsourcing. Staff changes still happen no matter what the organization is, and anyone can breach security. Chances are that an ISO supplier has more thorough

background checks and more strict hiring processes than any other organization.

BLENDED SOLUTIONS

If the organization is too small to hire its own security experts, then it has no real choice in the matter. But for bigger organizations, getting a second opinion about security is always good. Larger organizations are more likely to be attacked by outsiders. Any large organization should not only hire an inhouse team of security experts but also ISO suppliers to help with auditing, policy making, and additional security trends. The organization should not just hand over security completely, but work with a supplier to increase security. Benefits that come from having external eyes and expertise simply cannot be ignored.

One organization may find it very expensive to obtain experts, reliable data centers, 24-hour monitoring, hardware maintenance, software licenses, system upgrades, education about new threats, and critical security knowledge. Not only is this expensive, but some knowledge can come only from exposure to new threats after servicing multiple organizations. ISO suppliers should be used in conjunction with inhouse security. Information security is simply too important to ignore. A second set of eyes is always helpful when it comes to seeing security holes. Security leaks can come from anyone, not just from a supplier's employees. It is far better to have inhouse staff checking the suppliers and suppliers checking the inhouse staff. If security is completely trusted to one party, inhouse or outsourced, it can go on largely unchecked, creating more risks.

ENDNOTES

[1]"Losing Ground: 2009 TMT Global Security Survey." Deloitte, 2009 (www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/dtt_TMT-Security-Survey09-key-find.pdf).

[2]"Global Information Security Survey 2008." Ernst & Young, 2008 (www.ey.com/SG/en/Issues/Managing-risk/Information-security-and-privacy/Assurance---Advisory---Technology-and-Security-Risk---Global-Information-Security-Survey-2008).

[3]Kotadia, Munir, and Alex Serpo. "CIO View: Don't Outsource Your Security." ZDnet Australia, 1 November 2007 (www.zdnet.com.au/cio-view-don-t-outsource-your-security-339283433.htm).

[4]Conrath, Chris. "Panel: Do Not Outsource All Security." *Computerworld*, 3 June 2004.

[5]Evans, Bob. "Global CIO: The Ugly And Dangerous Prejudice Against Outsourcing." *InformationWeek*, 25 March 2009.

[6]Conrath. See 4.

[7]Fenn, C., R. Shooter, and K. Allan. "IT Security Outsourcing: How Safe Is Your IT Security?" *Computer Law & Security Report*, Vol. 18, No. 2, 31 March 2002, pp 109-111.

[8]Schneier, Bruce. "Why Outsource Network Security?" BT.com (http://globalservices.bt.com/InsightsDetailContentAction.do?Record=why_outsource_network_security_article_all_en-gb).

[9]Alner, Marie. "The Effects of Outsourcing on Information Security." *Security Management Practices*, Vol. 10, No. 2, May 2001, pp. 35-43.

[10]Schulz, Yogi. "Outsourcing Security Doesn't Always Add to Risk and Can Reduce Costs." itbusiness.ca *EDGE*, Vol. 5, No. 5, October 2006 (www.itbusiness.ca/it/client/en/Home/News.asp?id=41527).

[11]Schulz. See 10.

ABOUT THE AUTHORS

Justin Kim is a Network Analyst at Intelica Solutions. He is a former Senior Systems Integrator at iStock International/Getty Images. Mr. Kim has consulted with dozens of small and medium-sized businesses in Canada. He holds a master's degree in IS from the University of Melbourne. He can be reached at j.kim30@pgrad.unimelb.edu.au.

Sara Cullen is a Senior Consultant with Cutter Consortium's Enterprise Risk Management & Governance, Government & Public Sector, and Sourcing & Vendor Relationships practices. She is the Managing Director of The Cullen Group, a specialist organization offering consulting, training, and methodologies regarding commercial agreements. Dr. Cullen was a former national partner at Deloitte in Australia, where she ran the outsourcing consulting division. She has consulted to more than 110 private and public sector organizations, spanning 51 countries, in more than 140 outsourcing projects with contract values up to US $1.5 billion per year.

Dr. Cullen is a widely published author. Her publications include *The Contract Scorecard*, *Intelligent IT Outsourcing*, *Outsourcing: Exploding the Myths*, *Contract Management Better Practice Guide*, *Best Practices in ITO*, *Lessons Learnt in Outsourcing*, *Service Provider Management*, *Outsourcing Guidelines*, and *Outsourcing: What Auditors Need to Know*, in addition to research with various universities since 1994, including the London School of Economics, University of Melbourne, Oxford University, and the University of Warwick. She has been featured in such publications as *Australian Financial Review*, *Business Review Weekly*, *Computerworld*, *Directions in Government*, *European Journal of Information Systems*, *Information Economics*

Journal, *Journal of Strategic Information Systems*, *Information Technology Report*, *Insurance Directions*, *Oxford Handbook*, *MIS*, and *MISQ Executive*. Her expertise is globally recognized, and she performs peer reviews of outsourcing research for *Harvard Business Review*, *California Management Review*, and *European Conference on Information Systems*. Dr. Cullen has lectured at many universities, including the University of Seoul, the University of Melbourne, the University of Monash, the University of Swinburne, Queensland University of Technology, and the Royal Melbourne University of Technology. Dr. Cullen earned a BS in accounting from St. Cloud State University (US); she was awarded a master's of management (technology) from Melbourne Business School, and earned her PhD from the University of Melbourne. She is also a Chartered Accountant in the US. She can be reached at scullen@cutter.com.