Global Increase in Outsourcing Forces Organizations to Improve their Information Security Posture to Prevent Devastating Breaches by Eccuni

Article published on February 13th 2012 | Internet

Outsourcing of the Information Technology (IT) infrastructure is predicted to increase by almost 67% in the next 8 years. Companies across the globe are rushing to find ways to manage the information security risks and benefits of outsourcing. EC-Council's CISO Summit panel discussion suggests that increased information security compliance plans, continuous education, and knowledge sharing may prove to be the best solution.

February 13, 2012, Albuquerque, NM-Global economic troubles have motivated many companies to seek alternative means of conducting business that will cut costs and maximize profits. One of the most popular and effective methods is outsourcing of the Information Security (IS) infrastructure. According to a recent study commissioned by Savvis, Inc., this number is predicted to increase by almost 67% globally by 2020. IS outsourcing has its benefits; however, it often comes with high risk. EC-Council addressed the security challenges of outsourcing during a panel discussion at its CISO Executive Summit in December 2011.

"The challenges of outsourcing are similar to those you may have with the acquisition (insourcing) process. When acquiring a new company you need to ensure that due diligence has been completed prior to acquisition and integration, as you now will be responsible for the security of that company's data. This is the same with outsourcing," said Jeff Tutton, CISO Executive Summit Panel Chair and President of Global Security and Compliance at Intersec Worldwide, "Hire a trusted and qualified third party to complete a thorough evaluation of the outsourcing company. But don't just stop there. Put methods and controls in place to monitor and maintain the security of this data during the entire lifecycle. Trust but verify, and assign responsibility to a qualified person within your organization to manage and maintain oversight of security. Another option is to outsource only the data and systems that you want to end up in the public domain."

Tutton recently lead an interactive panel discussion centered on outsourcing and IS management at EC-Council's Inaugural CISO Executive Summit for Chief Information Security Officers. He was joined by Todd Bell, Executive IT Security Advisor, ConnectTech, LCC, Inno Eroraha, Founder & CEO, NetSecurity Corporation, Chris Oglesby, Senior VP, Knowledge Consulting Group, and Edward Ray, CISO, MMICMAN, LLC. The panel discussion addressed the challenges of managing risk and monitoring the outsourcing company's performance, while complying with recent industry changes such as SAS70 and PCI compliance. To view an interactive video of the panel discussion, please visit: https://www.eccouncil.org/ciso/resources

Tutton's panel discussion presented a detailed overview of the benefits and challenges of outsourcing in respect to Information Security. Globally, over 60% of organizations cite that managing the IT infrastructure domestically does not have any competitive advantages and are planning to move operations offshore. However, many offshore companies do not have the same legal restrictions as the United States. For instance, India, one of the biggest destinations for offshore outsourcing, does not have any data privacy laws. This lax in law enforcement leaves confidential information vulnerable to security breaches.

Last year, Epsilon, a cloud-based email service provider, suffered a security breach that ended up affecting around 75 clients and compromised over 60 million personal names and email addresses. Security breaches such as this can be extremely costly and detrimental to a company's reputation.

â€œIf an organization is looking to do a large infrastructure outsourcing engagement, the best way to ensure that security is a priority is to build a comprehensive list of security requirements into outsourcing contracts, develop appropriate service level agreements and reporting mechanisms to evaluate security and budget for a review by an independent assessment organization. This will ensure that security always stays top of mind," said panel speaker Chris Oglesby. â€œIf, however, the decision is to outsource infrastructure and security separately, then the security operations should drive the direction and outcomes and create independence between the organizations to meet the client needs."

In the future, companies need to employ executive IS leaders who will develop methods to adequately protect the IT infrastructure when outsourcing in-house responsibilities. Platforms, such as EC-Council's CISO Executive Summit Series, provide a means for top-level IS executives to gather and discuss the latest industry challenges. Continuous education and knowledge sharing will provide solutions to the quandaries top-executives face on a daily basis. For more information on upcoming EC-Council CISO Executive Summits, please visit: http://www.eccouncil.org/cisosummit.

Contact:

Marissa Easter â€“ Marketing Communications Specialist (marissa.easter@eccouncil.org)

About EC-Council CISO Executive Summit Series:

EC-Council CISO Executive Summit Series strives to unite the top Information Security (IS) leaders across the world in the fight against cyber crime and IS threats, while providing a platform for continuous learning where the most recent Information Security threats and landscape evolution can be discussed and debated.â€¬ Designed by EC-Council, the 1st in the CISO Executive Summit Series made its debut in Las Vegas, NV in December 2011. Due to the nature of the discussions, all CISO Summits are closed-door events open only to senior information security executives (C-levels, VPs, Senior Directors, etc.). http://www.eccouncil.org/cisosummit

About EC-Council:

The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in cyber security and e-commerce. It is the owner and developer of 20 security certifications, including Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), Certified Security Analyst /Licensed Penetration Tester (ECSA/LPT) and Certified Chief Information Security Officer (C|CISO). EC-Council has trained over 90,000 security professionals and certified more than 40,000 members. EC-Council's certification programs are offered by over 450 training centers across 87 countries. These certifications are recognized worldwide and have received endorsements from various government agencies including the U.S. Department of Defense via DoD 8570.01-M, the Montgomery GI Bill, National Security Agency (NSA) and the Committee on National Security Systems (CNSS). EC-Council also operates EC-Council University and the global series of Hacker Halted information security conferences.

Article Source:
http://www.articleside.com/internet-articles/global-increase-in-outsourcing-forces-organizations-to-improve-their-information-security-posture-to-prevent-devastating-breaches.htm - Article Side

Eccuni - About Author:

For more information about EC-Council visit www.eccouncil.org, follow @ECCouncil on Twitter, LinkedIn or visit EC-Council's Facebook page, a CISO Executive Summit, a Chief Information

Security Officers, a https://www.eccouncil.org/ciso/resources

Article Keywords:
Information Technology, information security, CISO Summit, Chief Information Security Officers, CISO Executive Summit, Certified Ethical Hacker, CEH, Computer Hacking Forensics Investigator, CHFI, Certified Security Analyst, Licensed Penetration Tester, E

You can find more free articles on Article Side. Sign up today and share your knowledge to the community! It is completely FREE!