SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

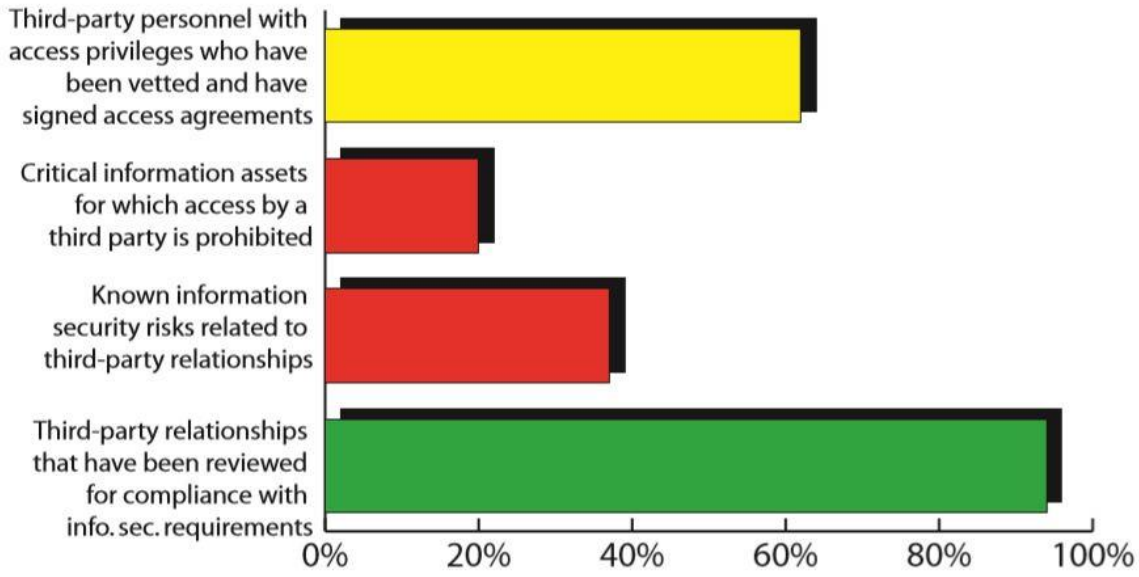
Security Metrics > Risk >

The Risks of Outsourcing Information Security

Created by George Campbell, Security Executive Council Emeritus Faculty

Outsourcing has become a fundamental business strategy for most major corporations. By outsourcing, businesses seek to gain an improved focus on core competencies and more profitable activities while reducing the cost of operations, obtaining specialized expertise and improving access to global markets. What they often overlook, however, are the risks that accrue due to the loss of effective business controls over sensitive activities — particularly those associated with the information infrastructure and vital information assets.

The following chart shows how one hypothetical CSO reports the current status of four basic controls for effective information risk management. Using data from an aggressive risk assessment program, this CSO wants to inform management and eliminate plausible denial. He or she can then urge action on current risk exposure while recommending a more focused risk management strategy going forward. The CSO also hopes to encourage management to adopt a more risk-focused due diligence process — one that proactively seeks out vulnerabilities and factors them into the procurement and post-contract oversight process.



On one hand, the chart above shows that the security strategy has been effective in driving requirements for background vetting (often resisted by suppliers), setting parameters on access to information assets, and performing risk reviews. On the other, the chart shows that more than a third of those with access have not been vetted, nor have they signed access agreements. Of greater concern are the findings that 80 percent of information assets allow third-party access and 37 percent of the known information security risks are related to outsourced partners.

Using this metric, the CSO can point out the known risks related to third-party relationships that are assignable to prior incidents and current risk assessments and can highlight particular findings of most immediate concern. For example, which of those unvetted non-signatories have access to the company's most sensitive data or critical elements of the infrastructure? Similarly, which of the company's most essential platforms, applications or data sets have failed to limit access, and what are the potential consequences of these vulnerabilities? Engaging business unit heads who "own" these relationships and determining answers to these questions will enable improved oversight and required mitigation tactics.

Where is the data? As shown on the green bar, fully 94 percent of the company's outsourced relationships have been risk assessed, providing a rich and timely database for determining the scope and nature of risk in this aspect of the corporate outsourcing program.

The CSO can also gain useful information if the security organization maintains an effective incident reporting and cyber investigation program that yields data related to risks assignable to third-party relationships. Engaging accountable business units in the

results of these assessments will also yield data on the potential risks associated with these findings.

Originally published in Security Technology Executive Magazine

Visit the Security Executive Council website for other resources in the Security Metrics > Risk series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com

Website here: https://www.securityexecutivecouncil.com/