Why Segregation of Duties Is a Must for SMBs + Best Practices and Policies

Devolutions

SMBS TYPICALLY HAVE FEWER CYBERSECURITY SPECIALISTS AND RESOURCES THAN LARGE ORGANIZATIONS

Today's hackers aren't just targeting enterprises and governments. They're also launching attacks against SMBs, and the reason is very simple: due to their relatively small size and limited funds, SMBs typically have fewer cybersecurity specialists and resources than large organizations. Two-thirds of SMBs have suffered a cyberattack within the last 12 months, 80% of SMBs say that malware has evaded their anti-virus software, and the volume and severity of cyberattacks against SMBs has risen during COVID-19. And the story only gets worse.

The Enemies Within

The same factors that make SMBs especially vulnerable to external hackers also make them susceptible to attacks from disgruntled or greedy employees/ex-employees, vendors, contractors, and other insiders. Of course, sometimes data breaches are the result of negligence, incompetence, or human error. But that's where Segregation of Duties (sometimes referred to as Separation of Duties) enters the picture.

What Is Segregation of Duties?

Segregation of Duties (SoD) is **a policy that forbids a single individual from being responsible for carrying out conflicting duties**. The goal, as highlighted in the ISO/IEC 27001 framework, is to reduce opportunities for either the unauthorized or unintentional manipulation or misuse of organizational assets. Basically, when multiple people are involved in a sensitive workflow, there is a smaller chance that anyone will try to break the rules, or for mistakes to go undetected.

SoD has been used for many decades in accounting, risk management, and financial administration. However, in recent years the concept has moved into the cybersecurity space. Its goals are to:

- Prevent conflicts of interest (real or apparent), wrongful acts, fraud, abuse, and the building of secretive "silos" around activities.
- Detect control failures, such as security breaches, information theft, and circumvention of security controls.
- Prevent errors from taking place due to employees wearing "too many hats".

SoD and POLP

SoD is rooted in the concept of the Principle of Least Privilege (POLP), through which end users are granted only the amount of access they need to carry out their jobs — no more and no less. While end users typically aren't thrilled with the restrictions imposed by POLP, the goal isn't to make anyone's life miserable. Instead, the purpose is to **minimize the size of the attack surface** and **reduce the likelihood and severity of a cyberattack**. This is especially important now that hackers are targeting compromised low-level accounts. Once they establish a foothold, they spread laterally across devices and networks, and ultimately access critical systems and sensitive data.

Best Practices

SMBs are urged to adopt the following SoD best practices:

- Conduct an internal audit, and **ensure that no single individual has unchecked and unmonitored systems access**. The exception to this rule in many SMBs will be SysAdmins, who legitimately require access to all applications, databases, etc.
- **Set up databases to align with task and role segregation**, which should be based on the Principle of Least Privilege (as noted above).
- Perform **ongoing information security audits and pay particular attention to potentially fraudulent activities**. SMBs that lack in-house expertise in this area are advised to work with an external firm or consultant, since malicious activity is almost always covert and difficult to detect.
- **Make it abundantly clear that audits and checks are being done**, such as regularly reviewing network logs. The mere fact that these verifications are in place will serve as a deterrent.
- **Provide end users with cybersecurity training**, ideally through an online platform. In addition to avoiding common mistakes and reducing errors, training fosters a culture of cybersecurity awareness and vigilance — which is a deterrent in and of itself.
- Implement suitable technology. For example, Remote Desktop Manager, Devolutions Password Hub, and Devolutions Password Server are all part of an information security infrastructure that supports SoD. Key built-in features include strong Role-Based Access Control, support for 2FA, and enhanced PAM functionality. All solutions are affordable for SMBs and available in a variety of licensing options.

Supporting Policies

In addition to the above, SMBs should implement human resource management policies that support a comprehensive SoD program:

- **Conduct pre-employee screening and continue ongoing screening** past the point-of-hire. The very existence of this policy will discourage employees from carrying out their illicit aims, or even working for the SMB in the first place.
- Train supervisors and managers to **recognize, document, and (as required) escalate any change in their subordinates' behaviors** and habits, such as an inexplicable rise in secrecy or nervousness when asked normal questions.

- If possible, force employees to take at least one two-week vacation a year. The irony is that in rare cases, an employee who seems very hardworking and rarely takes time off (more than a day here and there) may not be motivated by dedication, but instead is terrified of having their illegal acts exposed. Commented Jonathan Middup, a Partner at Ernst & Young's Fraud Investigation and Dispute Services Practice: "The profile of a typical fraudster is a long-serving, trusted employee, who works long hours and is reluctant to take their annual leave."

With the above in mind, it is important to note that the intent is never to create a culture of fear and suspicion. Truly, the vast majority of employees (as well as contractors, consultants, vendors, and other insiders) do not engage in any illicit activity and would never consider doing so.

However, SMBs do need to be proactive and watchful, because all it takes is one "bad apple" to trigger a potentially catastrophic outcome. The average cost of a data breach in an SMB is estimated between $120,000 and $1.2 million per incident, and 60% of SMBs go out of business within six months of a cyberattack.

From the Desk of Our CSO Martin Lemay

In addition to threats exposed by lack of SoD in this article, lack of SoD can also be similar to the "Single Point of Failure" concept for IT pros. Such a single point of failure should be avoided at all cost to reduce the magnitude of impacts in case of an unexpected behavior or failure. Keeping in mind that the top vector of an external threat is phishing, what would the impact be if the IT Director, assuming he has the keys to everything, gets caught? Security awareness is enough, you say? Your patch management is okay, you say? Would you jeopardize the survival of your business on those assumptions? I would not and I do not. There are plenty of other vectors that threaten this individual or an asset under their responsibility that could lead back to the individual compromise. The SoD threat model should be discussed and evaluated with senior executives, using a risk-based approach that aligns with business objectives. Is the impact of the compromise of a specific individual acceptable or not for the business? Not only from an insider threat point of view, but also as an attack surface? If the answer is no, perhaps it is time to split tasks and responsibilities to reduce threat exposure and impacts related to that individual.

A common caveat when applying SoD is – just like every IT problem that needs a solution – the tendency of overengineering the solution and producing undesired results. What if there is poor compliance and acceptance, business velocity reduction, rise of operational cost, and confusion over communication complexity? If hiring a new head count or more is considered JUST for applying SoD, it may be a sign that overengineering is taking place. As the business grows in maturity, however, natural delegation of responsibilities should take place and must not be constrained or limited for unjustified purposes. Compensatory controls could also be considered to cover the SoD weakness for the organization. Auditing, approval workflows, and other technological tools could help reduce such risks.

There are no golden rules for a good SoD scheme, but it must involve senior management in risk-based discussions with relevant personnel.

The Bottom Line

While SoD is not bulletproof (nothing in cybersecurity is), it significantly helps SMBs reduce their risk of being victimized by insider threats — which in some cases can be far more insidious, prolonged, and costly than attacks carried out by external hackers.