

## Four Security Pitfalls Facing Companies Today

### *Why Companies Aren't More Secure and How to Fix It*

Jeremiah Sahlberg, CISSP

***It is apparent that even today, security is an afterthought for many organizations.***

Following is a review of four pitfalls that organizations face and recommendations to solve them and improve an organization's security posture.

#### ***Pitfall #1: Insufficient Resources***

Companies need to budget for security. Similar to the software development lifecycle, security planning is more cost-effective to maintain than being purely reactive. Companies need to invest in a minimal set of employees and tools to establish and maintain an acceptable level of security and those investments need to align with business objectives. Some analysts claim that 5 – 10% of IT spend should be focused on

security, but each company is very different. Determining an amount should be reflective of the business model and exposure associated with the company's data assets.

Too often, companies do not approach security as a holistic process. Security often becomes part of the daily responsibilities of the IT staff that is already over extended by their day-to-day IT responsibilities. For example, a recent security audit conducted for a Fortune 1000 company revealed that only one employee was supporting security engineering and he doubled as a member of the IT support staff. When asked why patches were not being installed, the employee's response was, "there just are not enough cycles". Security costs need not be excessive, but should exist as a basic "utility"

***For more information contact us at:***

TekSecure Labs®  
331 Newman Springs Road  
Red Bank, NJ 07701  
Phone: (732) 833-5200  
Email: [info@teksecurelabs.com](mailto:info@teksecurelabs.com)

cost when defining the IT budget.

***Pitfall #2: Failure to Consider Security Implications***

Recently, a retailer was preparing for the holiday season and determined that they needed additional point-of-sale (POS) terminals to handle the “Black Friday” rush. The company quickly reconfigured each of its store fronts the week of Thanksgiving and implemented wireless capabilities to extend its POS capabilities to mobile laptops. When asked if a security review was performed in the planned deployment the answer was no. This could have exposed customers’ credit card information had the retailer not setup a secure wireless configuration. While businesses need to be able to quickly react to business demands to meet customer needs, the security “risk” needs to be part of the evaluation and decision making process. Companies need to continually ask, “What are the security risks?” Certainly all businesses need to balance the risk with the rewards and cannot achieve 100% ideal security, but all companies need to ask key questions to make the most informed decision. The criticality of this was demonstrated in 2007 when

TJ Maxx systems were breached by a weak wireless configuration at a single store in Minnesota and hackers were able to get into the headquarters database containing 47 million credit cards accounts.

***Pitfall #3 (and the most important) Failure to Follow the Security Lifecycle***

To successfully establish a security program, there must be a commitment to a holistic process. This process must be well defined, auditable, repeatable and measurable and must apply to all phases of the lifecycle. Additionally, there must be executive sponsorship of an overall strategy that clearly states the objectives and defines how to implement a plan to meet the technical, budgetary, and regulatory requirements. The challenge for organizations is how to implement these solutions in a budgetary-conscious manner. Whether the security roles align under the CIO or the COO, there must be sponsorship for a well defined process; otherwise the security program will fail.

***Generic Security Lifecycle***



Many security consulting companies utilize various circular or pyramid diagrams to represent the security lifecycle. While each is unique in how it requires more or less executive oversight and its need for security policy development, each has some core components from which any company can benefit.

Below is a traditional approach for implementing the security lifecycle.

**Lifecycle Step 1: Standards and Policy Definition**

Standards and Policy Definition step of the security lifecycle involves defining the strategy and policy by which a company will manage its security posture, as well as rules for the sequential phases of the security lifecycle. Creating a policy that affirms that the

company will comply with the Payment Card Industry (PCI) or adhere to other industry standards will allow an auditor to measure an organization's regulatory and security compliance.

### **Lifecycle Step 2: Assessments**

To perform a full assessment of a company's infrastructure, it is important to look at Internet-facing networks, internal networks, and the network architecture governing how those networks are structured along with the access controls that are in place for the network.

Web applications also need to be tested. Each business is unique and offers a unique way of serving its customers. A company will often deploy function-specific web services for B2B or B2C solutions. These critical custom applications are often created for their function and not by programmers with a background in secure coding; therefore these applications need to be tested for data leakage and data integrity.

With the availability of rapidly evolving wireless technologies, many companies have implemented WiFi capabilities, yet fail to evaluate the security of the WiFi

connections. The process of granting network access to remote employees, contractors and sub-suppliers needs to be reviewed so access is only granted to those authorized for such access. Also, once network access is granted, only authorized information should be accessible and then in a manner that does not expose protected data to the remote access worker.

Finally, the implementation of policies and cultural awareness is arguably the most important aspect of security assessments. A recent security assessment conducted by TekSecure Labs determined that adequate network controls were in place at the company's site, but the corresponding physical controls were not. In this assessment, TekSecure Labs security engineers were able to stand near a building entrance where smokers entered and exited the building. Using standard tailgating attempts, the security engineers were able to follow an employee into the facility unnoticed. The security engineers then proceeded to an executive's office and were able to take confidential documents before exiting the building, still unnoticed. The company's network security was rendered useless by employees being

unaware of their role in the company's security program.

### **Lifecycle Step 3: Prioritization/Categorization**

This phase of the security lifecycle includes understanding and documenting the critical data flow paths and information stores within a company and understanding how the identified security issues affect the business operations.

Once the security issues are clearly documented, remediation plans can be outlined. Typical actions may include the following:

- ◆ Remove the at risk component
- ◆ Update, patch, replace the at risk component
- ◆ Implement compensating controls
- ◆ Document issues deemed to be an acceptable risk to business operation

A common mistake of many organizations is that their IT staff will prioritize these decisions without consulting the business managers. An IT staff member may consider something an acceptable risk without knowing the overall business of an organization.

Several years ago, a web engineer commented it was acceptable to run outdated software since he tried to exploit a known vulnerability and couldn't, therefore, it must be secure enough. In fact, he told his Manager that it was secure. When questioned, he responded that since he could not get it to work and it was just one server on the Internet, "What is the risk?" While his question is valid, he did not have enough information to make a suitable decision. When TekSecure Labs demonstrated to this company that this SQL injection vulnerability could allow TekSecure Labs security engineers to delete all of the customers' records, it became apparent that there was a substantial risk to the business and with some additional security precautions that risk could be reduced.

This also validated to the company that security assessments need to be made by security experts who understand the latest tools and methodologies and that business decisions about what should and should not be implemented need to be made by those that fully understand the business.

#### **Lifecycle Step 4: Implementation**

Once a remediation plan has been developed, the appropriate remediation efforts need to be tested and applied.

Since the implementation of these security fixes typically fall on the shoulders of already overworked IT staff that have other "priority" projects in place, the implementation of security solutions needs to be defined as a top priority to ensure that the remediation activities effectively correct the identified deficiencies.

If a change is going to affect a production network, that change needs to be appropriately tested in a testing, development, or staging environment prior to production implementation. A mature organization will have in place a defined set of test case scenarios to validate that a change does not adversely affect a network, system or application. In some situations, failing to remediate an identified security issue may open the business up to even greater liability and risk due to negligence.

#### **Lifecycle Step 5: Validation**

When remediation is performed, it is critical that

someone validates that it has been implemented correctly. TekSecure Labs has consistently observed that a significant percentage of the issues that have been claimed to be resolved have not been resolved at all. For instance, it is not unusual for customers to apply the needed security patches, and then fail to restart the server so the updated fixes can be fully implemented. By performing the Validation phase of the Security Lifecycle, and providing the associated documentation, companies can measure their return on investment.

#### ***Pitfall #4: Failure to Perform the Security Lifecycle on a Timely Schedule***

One of the first questions that TekSecure Labs asks a new customer is when their last security assessment was performed. The answers range from "never" to "just last quarter" to "I don't know".

Technology changes every day and new security risks are being identified just as often. Waiting a full year to repeat the security lifecycle will not meet many customers' security needs. In fact, most customers are implementing a quarterly evaluation cycle for their most

critical and exposed Internet-facing systems.

Generally speaking, companies should have Internet scanning performed at least twice per year, while some companies may need it performed on a quarterly basis. However, performing a security scan from the outside is not enough. While this outside-in approach is important, an internal process for managing patches and system upgrades must be a continued focus for any company that wants to maintain a healthy security posture.

### *Summary*

#### ***Security is a journey— not a destination.***

New security issues are being identified and published every day. With the increasing diversity of technology and the steady rise in security issues on networks, operating systems and applications, it is important to keep security concerns as a top priority within an organization. Companies can realize an improved security posture and document their return on security investments by implementing an ongoing security lifecycle.

The most difficult task for an organization is to prime the security lifecycle “pump”. When a company’s security infrastructure has been neglected over time and there is no defined process for issue resolution, a company will have a reactionary response to security breaches which costs time and money that can far exceed the cost of implementing a robust security program proactively. By implementing a defined security organization, companies can fully understand their risks and make more informed decisions about how to mitigate those risks.

### ***About the Author***

Mr. Jeremiah Sahlberg is Director of Security Services for TekSecure Labs, a division of Tekmark Global Solutions LLC. Mr. Sahlberg manages the professional security service offerings of TekSecure Labs, which he helped found in 2002.

Formerly, Mr. Sahlberg was a Senior Security Engineer at Para-Protect Services Inc., specializing in information security consulting for top-tier clients. Mr. Sahlberg developed the web applications service at Para-Protect and his responsibilities included web applications testing, performing network penetration tests, analyzing system vulnerabilities, supplying incident response expertise and providing general security engineering work to clients.

With over 15 years of Information Security experience, Mr. Sahlberg has held positions in the government and private sector. Mr. Sahlberg led engineering teams and worked as a security engineer while employed by SAIC, Nortel and Defense Information Systems Agency within the Department of Defense.

Mr. Sahlberg earned a Bachelor of Science degree in Computer Engineering from Virginia Polytechnic University in Blacksburg, Virginia holds a CISSP certification and is a member of several professional security organizations. He actively contributes to the security community through publications on secure coding and web applications testing and has developed and maintains open source security tools.

### ***About TekSecure Labs***

TekSecure Labs ([www.teksecurelabs.com](http://www.teksecurelabs.com)), the network security division of Tekmark® Global Solutions, is a market leader in providing managed security solutions for businesses of all sizes and types. TekSecure Labs provides comprehensive network security, integrated managed services, and a portfolio of technology risk management solutions through a suite of products and services designed to ensure the highest level of network security for mission critical applications.

### ***About Tekmark Global Solutions***

Tekmark Global Solutions, LLC ([www.tekmarkinc.com](http://www.tekmarkinc.com)) provides information technology, telecom services, and business solutions to a broad range of Fortune 100 and Fortune 500 companies worldwide. Tekmark's client list is comprised of top companies in the telecommunications, financial services, technology, insurance, health care, pharmaceutical, and logistics industries, as well as county, state and city government. Tekmark's expertise lies in developing and integrating information systems, operating and improving technology and business processes, and helping clients evolve to the next generation of technologies. As one of the largest privately held technology and telecom solutions providers, Tekmark delivers innovative, cost-effective, results-driven solutions to help clients excel in their market place.