



# Security Risk and Overcoming IT Silos

By Alain Mayer

---

**The velocity of business and technology change and the disparate nature of the various function groups managing different aspects of the network create a risk environment that needs to be managed across the enterprise.**

Security risk is an unavoidable aspect of any IT infrastructure. Despite companies investing heavily in technology and operational processes to fortify their IT infrastructure, there will always be unintentional settings that expose business assets. The velocity of business and technology change and the disparate nature of the various teams and function groups managing different aspects of the network create this risk environment that needs to be managed across the enterprise. Often these function groups operate in isolation from each other, within silos of narrowly defined responsibilities that do not easily exchange information with other departments.

Most IT environments experience a high frequency of change which can compromise security and increase risk. Such change can be triggered by the following:

- Supporting new business services, e.g., rolling out supply chain extranets and moving server logic between internal network segments to data centers.
- Expanding functionality such as enabling guest deployment and corporate WiFi, adding servers to the DMZ, and enabling disaster recovery.

- Handling the increasing number of vulnerabilities in operating systems or applications that are continuously discovered and published, which leads to an increasing period between IT being notified about fixes and actually patching them. Diverse applications and operating systems need to be managed in the presence of frequent new patches and upgrades.

The problem with managing change is that it is handled by disparate, silo-oriented functional groups responsible for various aspects of the network such as:

- **Network device misconfiguration:** The firewall management group is mostly tasked with opening access through firewalls to enable business services. A simple firewall misconfiguration might allow Internet-based traffic to reach a credit-card database.
- **Software vulnerability:** The security management group typically does not scan all servers all the time. However, a database software installation with a new vulnerability might allow a remote attacker to obtain root access.
- **Server misconfiguration:** The server management group provisions new servers. A small oversight to re-

---

## The problem with managing change is that it is handled by disparate, silo-oriented functional groups responsible for various aspects of the network.

---

set password can result in a chosen password which is too weak to protect data on a server.

- **Missing patches/missing upgrades:** The application management group deploys servers to support business services. A slightly out-of-date database software installation might have a vulnerability that allows a remote attacker to obtain root access.

### How silos contribute to the problem

Security risk is not solely the consequence of an inexperienced IT staff or a lack of a mature process. Even with the most mature and best-trained IT staff, risk is unavoidable. The problem lies in the fact that risk is typically handled by a multitude of functional teams which prevents system-wide risk management and restricts operations down to more of a device-centric view. The following illustrates some typical silo situations.

#### Security operations group

This group applies a vulnerability scanner to most or all important servers, hosts and laptops/desktops, which typically generates a very long list of vulnerabilities. The security operations group then generates trouble tickets to hand off any remediation efforts. The challenge here is that it is not feasible to generate trouble tickets for all the issues reported by a scan. So, typically a limited number of tickets are issued for high-severity vulnerabilities on the most critical servers running the most important applications. But there is no guarantee that fixing only these vulnerabilities is reducing system-wide risk, as an attacker might exploit other vulnerabilities that are within his reach. This approach also creates unnecessary work if high severity vulnerabilities are firewalled off from any untrusted spaces.

#### Server administration or application management group

The server administration or application management group handles all software deployments, upgrades and configuration changes. Upgrades and patch deployments are often triggered by the trouble tickets issued by the security operations group. In turn, the server admin group issues change tickets to the firewall and network operation groups to support its mission of provisioning new services. Patching provides easily measurable units of work, but since most of the patching is triggered by the trouble tickets coming out of the vulnerability scans, there is no guarantee that actual risk is effectively

reduced. Furthermore, in some cases, no patch or upgrade is available for a given vulnerability.

#### Firewall management group

The firewall management group handles all changes to firewalls, including critical changes that determine what internal resources and data are accessible from the Internet, business partner connections, wireless access points, and other untrusted sources. These changes come from a variety of places, sometimes triggered by incoming change tickets from the server admin group or application managers. Typically these change tickets are for opening up access, but once access is open, seldom does the firewall group have the resources to monitor all business services to make sure they should be left open. The firewall group itself does not have the application blueprint needed to determine what existing access should be closed down if a business service is terminated. This group is often reluctant to participate in risk-reduction tasks except for obeying simple, device-centric security policies. Such policies are not sufficient to effectively manage system-wide risk.

#### Network operations group

The network operations group handles all changes to network devices such as routers, switches, and load balancers and is responsible for ensuring availability and connectivity for business services. Network device changes are often triggered by change tickets from the server and application management groups. With a primary mission of assuring connectivity, sometimes the application team can change the access requirements that exposes another portion of the corporate network.

It is easy to see that even in a mature operations environment this silo-based, device-centric approach can be wasteful and not effective in reducing risks that affect the business. Every operations group is focused on separate tasks. These separate tasks get prioritized according to each group's objectives. These groups seldom have the visibility or the knowledge to understand the system-wide impact of their actions on business risk, thus inhibiting effective security controls.

### Steps to reduce risk

Despite these typical organizational and functional boundaries, it is possible to reduce risk. By considering all steps within reach of all operational groups, it is possible to increase effectiveness of a risk management program while reducing the overall effort. Among the actions that can be taken are the following mitigating responses that today are handled by separate groups and that, due to time constraints, are often done in a vacuum.

1. Increase the strength of protection for the host/network
2. Patch a given host/device to eliminate the vulnerability
3. Patch the upstream host that is exposing this host

4. Change the configuration of the susceptible host to eliminate the communication path
5. Change the network access/configuration to eliminate access to the host
6. Protect the host using an inline security mechanism

The countermeasure to the silo-approach is to evaluate the above mitigation options from a system-wide context. Establish a centralized security team, whose mission is to establish and maintain an IT security blueprint. Such a blueprint is the basis for assessing all exposures across all functional areas of responsibility, which then leads to a natural prioritization of exposures and a common risk assessment. Such a common focus leads to more effective mitigation tasks for each operations group, allowing the groups to leverage each other's work and arrive at acceptable levels of security risks.

More concretely, here are some of the steps to establish a common security blueprint:

### Step 1: Risk prioritization criteria

1. Determine which hosts and vulnerabilities can be firewalled off. This requires the input from two separate sources, typically managed by two different teams: (1) the current vulnerabilities, and (2) the current network paths from the Internet to hosts and ports that expose these vulnerabilities.
2. The centralized team, responsible for maintaining the system-wide network blueprint, establishes which hosts are exposed through a network path to untrusted sources and have corresponding vulnerabilities. These processes, which ideally are automated, should yield prioritization criteria for mitigating risk.

Example: Buckets can be created (1) for hosts that are network-reachable from the Internet and have high severity vulnerabilities, (2) for hosts that are network-reachable from an extranet connection and have high severity vulnerabilities, and (3) for hosts that are network-reachable from a wireless access point and have high severity vulnerabilities. More granularity can be obtained by classifying high-severity vulnerabilities into those that can be used as stepping-stones for attacking deeper into the network or by classifying hosts based on information from asset management systems according to compliance or other criteria.

### Step 2: Risk Evaluation Process

1. Conduct regular meetings with network and server teams to determine how vulnerable hosts can be blocked instead of being patched. Using in-line technology, such as application firewalls, network IPS, and an inline patching system, the patching cycle can be optimized with the server service window while maintaining application availability.
2. Conduct regular meetings with the network team to review what "perimeter access points" may create untrusted access to the network and which ones are attached to vul-

nerable hosts. These perimeter access points include the Internet, partner extranets, wireless access points, and new networks segments. You should pay closer attention to host vulnerabilities attached to these access points since attack sources could show up on these points and gain access to your network. For example, a host with a low priority vulnerability may be on a guest wireless network. If this host has access to the internal network, then it is important to eliminate this host as a "risk" by either patching it or blocking its access to the internal network.

## Conclusion

Security risk management has lagged behind other security disciplines because most IT departments do not have a cross-functional commitment to analyzing the impact of change on the system-wide security posture. The challenge of effectively managing risk is gathering data that provides situational awareness and visibility into security postures from a myriad of sources, managed by functional IT silos, including network devices, systems, applications, and vulnerability scanners. Once this information is gathered, it needs to be automatically analyzed and correlated system-wide to identify and prioritize the steps needed to reduce the risk for the company.

Ever changing business, technical, and security environments place tremendous pressure on the IT operations team to deliver highly available services while minimizing the security risk to the company. While risk is an unavoidable aspect in any IT infrastructure, and each functional team within the IT operations group (security, server, and network operations) has their own perspective on how to minimize risk, it is easy to see how this silo- and device-centric approach can be wasteful and less than effective.

Risk can be reduced by considering the steps within reach of all operational groups and agreeing upon a system-wide prioritization scheme to enable the most effective way to mitigate the risk while balancing the uptime of the critical business services. Taking this perspective can reduce risk while reducing the overall workload of the IT team.

## About the Author

*Alain Mayer, CTO of RedSeal. Alain's 18 year professional career includes research and development in areas such as algorithms, compilers, network protocols, and computer security. Prior to co-founding RedSeal Systems, Alain was the CTO of CenterRun, a data center management company that was successfully acquired by Sun Microsystems. Alain is a recognized researcher whose work has been awarded the USENIX "Best Paper Award in Security, 1999" and USENIX "Best Paper Award in Electronic Commerce, 1998." Alain earned a PhD in Computer Science from Columbia University. He can be reached at [alain@redseal.net](mailto:alain@redseal.net).*

