

Complexity: Addressing the big threat to your organization

By Joel Weise

Complexity is one of the most critical – if not the most critical – threats facing organizations today.

The networks of the future will be necessarily more complex, and therefore less secure.

– Bruce Schneier,
“A Plea for Simplicity”

Complexity is one of the most critical – if not the most critical – threats facing organizations today. This is not to suggest that phishing, hacker attacks, viruses, malware, terrorism, natural disasters, organized criminal gangs and even poorly trained staff or inept insiders are not real or in fact costly threats to the enterprise today: They are. In fact, according to Bruce Schneier, “The worst enemy of security is complexity”¹. Although complexity is at least equally real and costly as these other risks, it is often overlooked amongst them. A complex or overly bureaucratic organization is not as easy to manage, and this leads to greater costs, greater risks and a decreased chance for success. Bureaucracies by their nature are often chaotic, because typically they accomplish so little – the end results are the same for chaotic and bureaucratic states. This article explains why complexity is a key architectural design problem, one that introduces serious business and technical risks; and it explains how to use adaptive security to address these important issues.

What is complexity?

So what does complexity mean? Often the term is used to refer to intricate or compounded systems that are meshed or entwined and may include an overabundance of variables. (This definition is based in part on the original Latin *complexus*, or “embracing.”) This article takes this fundamental definition and extends it into the context of the IT world. For the sake of this discussion, complexity is considered a characterization of a system and its components, i.e., people, processes and technology. Therefore, a process or situation may be complex, just as an IT infrastructure may also be complex. As such, any process, situation or task that reduces the effectiveness of controls, increases costs, reduces operational effectiveness or reduces productivity may be considered complex.

Simply stated, complexity is the opposite of simplicity, and the goal for every IT organization should be to increase simplicity, thereby reducing complexity, chaos, disorder and entropy. Increasing simplicity creates harmony, order and homogeneity; but this is not meant to suggest that all systems must be mirror images of one another. Rather, they work together in concert, in a holistic and synergistic manner.

To what does complexity really correlate? Of course, complexity affects more than just security. As more demands are made on people, process and technology, complexity tends to increase, and tends to magnify or multiply problems and threats. It adversely affects those characteristics which a high-performance organization exhibits, whether those might be missing service levels, or the CEO being indicted for not complying with a new legal mandate. Complexity is also compounded over time: As time goes by and the contributor factors add up, the level of complexity, chaos and entropy will get worse. If the level of complexity overcomes an organization’s ability to maintain the characteristics of a successful organization, as noted below, then the organization is doomed – or relegated to an inferior business position amongst its peers.

Contributors to complexity

It is clear that complexity permeates many enterprises, from application and system development to operations and systems management. How often has a project gone over budget and come in late, or even a “simple” system change turned into a three-day-and-night, back out and restore event? What amount of training is required to enable staff to work competently with a new procedure or application? How often do staff attempt to bypass policies and procedures because they are perceived as too complicated, or “they get in the way of us doing our job”?

¹ <http://www.schneier.com/essay-018.html>

These problems do not typically occur because of poor security or external threats; rather, they occur because of factors such as:

- Unnecessarily complicated business and technical policies, procedures, operations, applications and systems, which often are not understood, read, or kept up to date
- Poor understanding of business and technical issues when these policies, procedures, operations, applications and systems are designed and developed; presenting the additional problem of management, maintenance and repair
- Attempted integration into poorly understood systems, including legacy systems designed by long-gone staff
- Lack of adequate and appropriate documentation
- Lack of applicable standards and guidelines
- Lack of interoperability, forcing difficult workarounds
- Poorly understood legal and regulatory mandates
- Poor quality assurance and change control processes
- Non-unified approach to compliance. Compliance to convoluted and conflicting regulations is difficult at best
- Difficult and invasive processes and procedures, which will be ignored
- Policies that are too strict (e.g., a too-strict password rule is difficult to follow). Don't get in the way of people doing their jobs by adding overly restrictive procedures
- A large volume of data that can overwhelm a system, resulting in degradation of performance and increased storage/retention costs
- Use of incoherent, obsolete and/or incompatible protocols, interfaces, processes, applications and systems
- New and poorly understood technology; e.g., using new technologies the way you used old technologies, and thus not taking advantage of new features in the new technologies
- Lack of governance across the organization, for business and technical processes
- Conflicting political agendas within the organization. Too many chefs, all claiming to be owners or experts, create organizational inertia and inhibit forward progress
- Too many variables, options, configurations and parameters at various layers of abstraction: hardware, OS, networking, middleware, application and management
- Insufficient levels of the characteristics noted for successful organizations

Addressing complexity

Complexity occurs in organizations that do not implement a comprehensive security effort, or do not properly fund, promote or consistently manage the efforts they do implement. Complexity further occurs in organizations which allow operational processes to deteriorate such that they cannot keep up with changes in the competitive business, legal and regulatory environment within which they must operate and compete. This article will make some simple recommendations for addressing complexity, and further describe the characteristics of a high-performance enterprise that is able to address complexity and also maintain its competitiveness, increase its

market share, retain and attract more customers, and in general, be successful.

An example of a definition for a high-performing organization can be found in the work of the Information Technology Process Institute. *The Visible OPS Handbook* states:

“Based on our analysis, we have created the following working definition of high-performing IT organizations: They are effective and efficient and they succeed in applying resources to accomplish their stated business objectives with little or no wasted effort. These organizations have evolved a system of process improvement as a natural consequence of their business demands. They regularly implement formal, repeatable and secure operational processes”².

Given this definition, it can be stated that a successful organization (i.e., one that reduces complexity) ensures that it maintains cost-effective and appropriate levels of the following characteristics:

- Availability – your data and processing resources are there when needed
- Reliability – your data resources are correct and accurate
- Agility – you can implement changes faster than your competition (and also respond faster to a changing business and technical climate)
- Operational efficiency – you can run your business faster and cheaper than your competition
- Security assurance – confidentiality, integrity and privacy are supported, such that your data resources cannot be disclosed or modified without authorization
- Accountability – people are responsible and perform their jobs

All of these characteristics are complementary to security, and when optimized will reduce the level of complexity in one's enterprise. The reduction in complexity is accomplished by utilizing an adaptive security architecture in conjunction with a security maturity model. In other words, organizations with satisfactory levels of these characteristics will find the level of complexity in their environments reduced accordingly.

There is a specific recommendation for directly addressing complexity. To support the above characteristics and reduce complexity, use adaptive security techniques coupled with a security architecture and security maturity model.

Adaptive security

Adaptive security is an integral security effort that allows an organization to implement controls capable of responding to new and different threats over time. The primary differentiators of an adaptive approach to security (versus, say, a prescriptive or checklist approach) are agility and resiliences. In addition, adaptive security implements a security architecture that matures over time to anticipate evolving threats. The security architecture is designed, implemented and managed within the context of a continuous improvement schema, so that the characteristics noted above are supported, and complexity thus reduced. In this way the organization utilizes security as a vehicle for innovation that focuses on driving predictive and proactive change, and utilizing a dynamic security architecture as well as operational processes and controls. Note that a security architecture can be utilized for new environments or applied to existing infrastructure.

The security controls built into an IT architecture will be made to include such characteristics, and in particular to provide traditional security assurances of identification, authentication, authorization, auditing and monitoring, confidentiality, integrity, and non-repudiation. Further, such architectures naturally support time-tested security principles such as defense-in-depth, compartmentalization, least privilege, and proportionality, where necessary and possible.

This is an example of a security maturity model.

Level 1 – Chaotic Security

At Level 1, an organization's security capability is best characterized as immature or chaotic. The organization is exposed to substantial liability. There has been little effort undertaken towards creating and sustaining a secure and compliant IT environment. Investment has been minimal, and any organizational IT security success thus far has been achieved solely through the efforts of heroes. Activities, if any, are focused on the security needs of individual projects or elements within the IT infrastructure. The organization is reactive and often left to rely on firefighting activities after security, privacy or compliance problems are discovered by IT users, auditors or customers. Level 1 is reached when IT shows up for work in the morning.

Level 2 – Basic Security

At Level 2, some investment has been made in the area of IT security, although such investments tend to focus on specific projects or problems, often utilizing point solutions that are not guided by an overall integrated vision and strategy. The organization is still exposed to substantial liability.

When needed, IT security policies, processes, standards and controls can be found, though often they are not widely and consistently developed, communicated, implemented or managed. Core IT security policy, processes and controls are beginning to be formalized in some fashion, but this effort is still very much in the formative stages. The level of IT security throughout the environment is still inconsistent, due to the fact that most of the policies and processes are not defined, and those that are defined may not be consistently implemented and audited. Most organizations reach Level 2 without structured, systemic efforts to address IT security and compliance problems.

Level 3 – Effective Security

At Level 3, the organization has begun to realize the strategic, competitive and regulatory advantages of developing and maintaining a consistent IT security posture throughout the environment. Organizations will develop a security, privacy and compliance vi-

sion and strategy, as well as a plan that will serve as a transformational roadmap to help the organization achieve its IT security and compliance goals. Organizations at Level 3 are characterized by a more proactive approach to IT security with respect to infrastructure, applications and services. Such organizations have developed and applied (more systemically) product, capability and configuration standards. They may also have started to streamline their IT security management practices through the use of automation technologies for both control and assessment. The security of the environment also grows stronger as IT security processes become more repeatable and audited for compliance. Reaching Level 3 requires that an organization have an epiphany regarding the nature of, and solutions for, its IT security and compliance problems. The realization is that ensuring the secure delivery of services and the protection of IT assets requires a holistic approach that addresses the environment systemically from the perspective of policy, people, process and technology.

Level 4 – Optimized Security

At Level 4, the IT security capabilities of the organization are measurable, predictable and repeatable, liability management is in equilibrium, and all security requirements have been addressed, where appropriate, through the implementation of an integrated security architecture.

There is a clear IT security and compliance vision and strategy from which projects, policies, processes and control are derived. There is a well-defined governance process for engaging IT security in the service development and information protection lifecycle. IT security can be consistently measured and managed in accordance with well-defined metrics, policies and service agreements. Greater levels of efficiency and optimization are achieved through the use of automation and continuous refinement practices. Failures as well as lessons learned are viewed as an opportunity to improve IT security, and are consistently used in the development and refinement of policy, processes and controls. Reaching Level 4 generally occurs when the organization shifts

Security maturity model

The use of a security maturity model allows an organization to develop a security architecture that evolves iteratively over time. This approach also allows for a roadmap to be developed to direct the elaboration of a security architecture as it responds to new threats as well as new business and technical requirements, e.g., new legal mandates, tighter service levels, availability of faster and cheaper compute platforms, terrorism and even higher energy prices.

from being an IT security operations organization to being a secure, compliant service delivery organization. Liability management is in equilibrium, i.e., the organization has achieved compliance to all applicable legal, regulatory and other mandates as necessary. In addition, accreditation and/or certification have been obtained with applicable standards and industry best practices (e.g., NIST, Common Criteria, FIPS 140-2, ISO 17799, ISO 27001).

Level 5 – Adaptive/Dynamic Security

At Level 5, the IT security organization has moved beyond addressing liability issues and the implementation of an integrated and holistic security architecture, and is focused on continuous process improvement, adding quantifiable value to the business. The data available from the management and support infrastructures is used to modify processes in order to gain efficiencies. With each security challenge or failure, the organization learns and grows safer, stronger and more compliant. Traceability from the business metrics to the IT security metrics allows decisions and process improvement in one area to be based on information from another. Security, risk and compliance decisions are now more grounded in facts rather than conjecture, leading organizations to more wisely and efficiently use and secure their IT assets. Further, innovation is now more readily possible. IT security, at Level 5, is already leveraging automation, and has been optimized for the business. IT security innovation will therefore often focus on driving predictive and proactive change through the use of adaptive and dynamic security architectures, processes and controls. Adaptive architectures allow the organization to respond in a more agile manner to "just in time" business opportunities, all the while ensuring that a compliant IT security posture is maintained throughout service development and delivery lifecycles. Adaptive security can be used to construct self-defending architectures that are not only resilient to attack, but also able to adapt in response to new security requirements or threats.

The goal of security maturity modeling is to help organizations move from more basic security structures to those that are more sophisticated, agile and responsive, in order to better manage risk, cost and complexity while at the same time improving availability, performance, integration and, of course, compliance and security. Organizations at a fundamental immature stage (Levels 1 or 2) are typically at much greater risk than their peers, who may be operating at more advanced (Levels 2 or 3) or strategic (Levels 4 or 5) phases, where a comprehensive security architecture and process structure are firmly in place, functioning well and continuously improving over time.

An example of a security maturity model appears above.

The use of common industry best practices and nationally and internationally recognized standards will also help reduce complexity. For example, the use of standardized hardware and software protocols, interfaces and computing languages will reduce inherent complexity by allowing for the use of abstraction layers that mask complexity. With abstracted protocols and interfaces, virtualization can occur, resulting in cost reductions, simplification of operational processes (e.g., via automation and easier provisioning) and optimization of resource utilization.

Conclusion

The benefits of using an adaptive security architecture and maturity model are that an organization can reduce complexity, chaos and costs, and become more agile, operationally efficient, productive and secure. Further, such an organization is more responsive to changes in its business environment, as well as the legal and regulatory mandates promulgated over time. As can be seen in the Visible Ops definition of a high-performing IT organization, responsiveness to change is critical to a successful organization, and likewise necessary to keep complexity in check.

In the absence of an effective, comprehensive and consistent security architecture and maturity model, applied throughout the organization, organizations find themselves strapped with ineffective, unmanageable and overly complex environments. They will be at greater risk to various threats than organizations which have a more effective security posture. It must always be remembered that attackers normally take the path of least resistance and attack the most vulnerable prey.

As the above descriptions show, each organization should develop a security architecture based on an adaptive security approach, coupled with a maturity model targeted specifically for the organization. Such an approach will provide a means for defending against

malicious attackers, reduce errors by poorly trained staff, enhance compliance and governance, and improve the systemic qualities of availability, reliability, agility and security assurance.

About the Author

Joel Weise has worked in the field of information security for over 25 years. As a Principal Engineer for Sun Client Services, he designs system and application security solutions for a range of different enterprises. Joel is the Sun Microsystems ANSI representative, a member of the ISSA Journal Editorial Advisory Board, a member of the Sun BluePrints Merit Review Board, and author of various Sun BluePrints.

References

- Behr, Kevin et al., *The Visible Ops Handbook: Implementing ITIL in 4 Practical and Audit-able Steps*. Information Technology Process Institute, 2005.
- Schneier, Bruce. "A Plea for Simplicity." November 19, 1999. <http://www.schneier.com/essay-018.html>