MARCH 2015

BUSINESS TECHNOLOGY OFFICE

Protecting the enterprise with cybersecure IT architecture

As digitization creates new cyberthreats, businesses should make security an integrated part of their IT infrastructure.

Oliver Bossert, Wolf Richter, and Allen Weinberg

Digitization of data, products, and processes is an increasingly important driver of economic growth, but it also creates a host of cybersecurity challenges and vulnerabilities. The push toward greater multichannel integration, for instance, adds significantly to the customer experience but introduces many more interfaces that intruders can exploit. Likewise, companies' closer collaboration with business partners, customers, advisers, and other third parties can enrich everything from product development to recruiting but can also result in more complex, conjoined supply chains and information flows. Hybrid delivery models, in which some business services and processes are moved to the cloud and managed by external providers, extend the security perimeter and add to the sweep of activities that companies must monitor to detect attacks on their environments.

Not only does digitization introduce more openings for hackers and others to exploit, but it also increases the value of an organization's data assets. Within the banking sector, for instance, the use of big data and analytics may greatly increase a bank's ability to target and serve high-value clients with specific cross-selling offers. The value of the data rises as customer information is aggregated and cross-referenced—allowing companies to track names, demographics, and purchase histories (with due regard for customer privacy)—but so does the attendant risk. A breach can expose the bank and its clients to severe financial and reputational harm.

IT organizations should help the business take advantage of robust analytics capabilities while also ensuring that the information and application architecture adequately protects sensitive data. The trouble is,

Takeaways

Many companies' approach to cyberrisks emphasizes building walls that can add complexity and increase vulnerability.

Instead, putting in place secure enterprise architecture, which treats security as a basic design principle, can help.

Analyzing the value at risk from potential breaches and using multiple layers of defense to guard against threats offers a flexible approach that will serve businesses as their priorities shift.

they're in a race against time. A joint study by McKinsey and the World Economic Forum in 2014 revealed that 71 percent of global banking IT executives believe that attackers will continue to move faster than banks in modifying their skill sets and spotting potential vulnerabilities. Additionally, 80 percent of respondents believe that the risk of cyberattacks and compromised data will have major strategic implications for their businesses over the next five years.

To stay ahead of attackers, companies need to design processes, platforms, and IT infrastructures with security in mind and incorporate secure architecture principles into their security programs.

Limits of existing architecture

Many organizations have invested heavily in IT security, but because of budget and time pressures, most have ended up layering new security infrastructure on top of their existing IT architecture. That creates a heterogeneous architectural landscape in which individual systems are haphazardly ring-fenced. Sorting that out increases the need for manual intervention and vastly hinders system updates. Instead of resulting in a more secure architecture, this piecemeal approach to IT security often creates greater complexity and unanticipated gaps in a company's cyberdefenses.

What's more, the pressure to launch digitized services quickly can introduce other challenges. The rush to roll out automated, end-to-end process work flows through the cloud can sometimes result in poorly planned pilots that are coded without considering how they will be integrated into the existing landscape. Companies that proceed without first creating a safe testing area, or "sandbox," can end up putting their entire IT landscape at risk.

Elements of secure architecture

Secure enterprise architecture is an approach to IT security in which security is treated as a basic design principle of the architecture rather than as an additional layer. It includes several principles.

Alignment of business domains and security requirements. Traditional IT architectures are oriented along business domains that are based in some way on business processes. For a retail company, for instance, these domains might include the supply chain or store management. By contrast, a secure IT architecture reflects both the business processes and the risk exposure of the assets and processes in each domain. Security is built into the definition of the architecture and is therefore an integral part of it. Rather than increasing complexity, security is inherent in the architecture itself.

Grouping by capability. Similar process activities are grouped at the capability level, such as customer management or account management, to make the architecture manageable as well as secure. Each capability is assigned to a business domain and a security domain. The capability level is used to assess the risk exposure of assets

and processes and to specify adequate and consistent levels of security requirements. These requirements are defined in security domains to enable homogeneous levels of protection for assets with a similar risk exposure across the architecture.

Modularity. The security level of one security domain can be adjusted without affecting the security levels of other domains. The modular structure allows organizations to adequately measure the risk exposure and protection need of each capability across the respective business domains. Monitoring technology can be deployed at pivotal points within the infrastructure to increase the level of security. Merely securing the connecting points between the corporate network and the public Internet is not sufficient. Insider threats are growing in importance, and the most advanced adversaries have devised attack methods in which they penetrate a network in multiple small steps over a period of weeks or even months—steps that remain invisible to the outside guards: think of bringing dismantled weapons into a guarded city piece by piece. These attacks can be detected only by constantly observing the activities inside the network and installing alert systems that can detect small changes in user activity. Dividing a network into security domains has two advantages. First, it creates clearly defined borders inside the network at which traffic can be monitored. Second, changes in activity within one domain with a more limited set of applications are easier to monitor than lots of minor changes across the whole network.

Consistency throughout the stack. Security requirements propagate and are aligned across the stack from the capability level to the IT infrastructure level. Management tools allow organizations to monitor and manage the mapping across different layers and maintain transparency across the IT organization and infrastructure.

Integration across the supply chain. Using defined security domains and mapping assets (for example, the customer database) to them end to end allows organizations to engage business partners in determining the appropriate security requirements for each cross-organizational information flow. This also serves to reduce the number of point-to-point links and drives trading-partner integration through well-defined and more easily protected APIs. While that may seem like an additional layer of complexity, such attention to detail is a necessity when negotiating supply-chain integration, since attackers will always look for the weakest link in the chain.

Moving toward a secure architecture

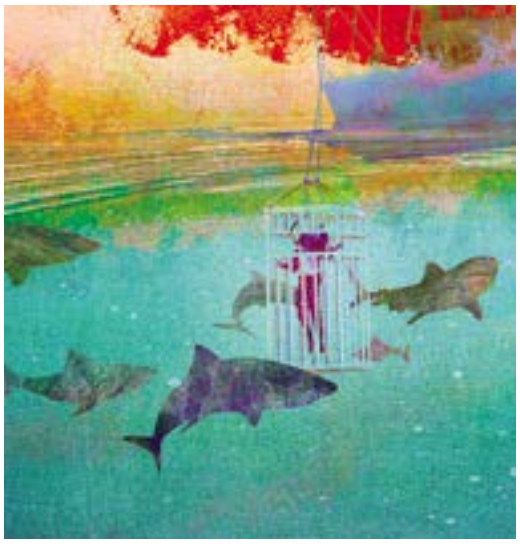
Secure enterprise architecture begins with an initial security assessment to identify and isolate capabilities by threat level. The

assessment goes beyond identifying gaps in defense; it also involves analyzing the most critical business assets, such as proprietary trading algorithms or underwriting data that, if compromised, could result in material losses and reputational harm.

Threat-based isolation separates high-value and high-risk assets and processes from low-value and low-risk ones while still allowing organizations to take advantage of shared infrastructure and virtual environments. High-value financial transactions, for instance, can be processed through a separate authorization engine, and an online banking portal can be made to run on different applications and servers from those for the bank's public website. The data and process steps that support these activities are grouped under discrete capabilities, such as online account opening or money transfer. A "business back" analysis of the value at risk determines an adequate level of protection and links the resulting grouping to a security zone in the architecture. The value at risk can be determined by estimating the operational, reputational, financial, competitive, and regulatory impact of a breach. The value at risk also considers the downtime of a process because downtime can lead to regulatory fines, for example, for negligent handling of customers' personal information.

We call this approach "castle architecture," for its multiple layers of defense, including the following elements.

1. A 'castle keep.' Segregating threats according to the value at risk places the company's most valuable assets within the most secure domain, access to which is highly restricted. Valuable data assets such as these would come under strict master-data management. No data with a security rank of "confidential" or higher would be stored on mobile devices. Laptops would employ virtual clients with no local data storage. All classified information could be retrieved only from the master-data database on demand by authorized systems, and all access would be monitored. Assets with lower value or risk can be housed in more accessible layers with appropriate levels of security. The importance of multiple defensive zones was illustrated by a recent assessment of the infrastructure of an insurance company. The assessment showed that more than 80 percent of the company's applications contained assets with high value at risk, which indicates a high level of vulnerability should an attack take place.



2. Defense in depth. The interlocking layers of security we describe function as defense perimeters. With each layer, access becomes increasingly restricted, and information on unusual events is tracked. Inner layers of security are tightly integrated. Sensors and

logging mechanisms monitor the outer perimeter and important applications within the network. Database trails are also recorded and analyzed in near real time to detect unusual access patterns, while auditing engines monitor database transactions. A leading wealth-management company was able to trace the fraudulent use of online accounts back to an employee who had left the company more than three years earlier by analyzing records and narrowing down the search scope to a few people who would have had access to specific accounts.

3. Service architecture. Service architecture is an effective means for managing different levels of security within individual business domains. Data and process steps are encapsulated in services (for example, validating a customer's credit-card information) such that each service effectively creates a perimeter within each domain. Since each capability is modeled as a service from an architecture point of view, companies can better monitor the flow of data across the network. For instance, all communication goes over defined service interfaces and a common bus, with services classified according to their security requirements. Service-based architecture secures each asset with a private ring fence.

4. Common bus communication. By routing all communication among the services through a common application service bus, companies can effectively monitor the flow of information. Large-scale pattern-recognition tools can be introduced to detect suspicious changes in communication patterns. Most companies have defined patterns that they consider suspicious. But in order to detect such patterns, the monitoring devices need to be able to process data from all parts of the IT landscape. Strict enforcement of bus communication cuts across all direct connections between applications. This secure approach will become an imperative in future enterprise architectures; at the moment, a large part of major IT system landscape architectures is still characterized by direct connections between applications, mainly for performance reasons. CIOs must now accept that cleaning up the legacy landscape and introducing a modern bus and service architecture is part of their mandate.

5. Standardization and simplicity. Secure enterprise architecture fosters an environment in which interfaces, technologies, and cross-sectional functionalities are standardized and harmonized, the number of interfaces is minimized, and data flows are clearly structured. One application service bus handles all messages between applications, and one consistent role-based authentication and authorization system is used for employee access. The variety of end-user devices and operating-system versions on the network is minimized, and the number of different database engines and software versions is strictly limited. Clarification of all interfaces with the database enables the detection of suspicious operations. Introducing strict security audits for nonstandard devices and technologies and providing preapproved solutions as services to the organization are prerequisites to drive standardization.

6. Innovation 'sandboxes.' Companies need the ability to build and deploy software rapidly to support everything from new

campaigns to product development. A heavily shielded "development sandbox" can provide an appropriate safe haven for new projects and experimentation. Creating such sandboxes is one way digital leaders can carve out space for innovation while maintaining the transactional back-end systems that keep the business running. We call this "two-speed architecture."[1] While two-speed architecture is mainly discussed using the lens of faster time to market or greater customer intimacy, security is becoming a decisive argument to move toward a zoned or multispeed IT landscape.

The transformation journey

As a company moves toward a secure enterprise architecture, it must start with a clear vision of the target state, a solid road map for getting there, and a culture of change that supports the journey.

Arriving at a vision. A business-driven secure architecture can only be developed in parallel with the business strategy. That strategy must emerge from discussions led by the CIO and business leaders and should be translated into a target capability map and systems manifesto.

Creating a road map. Heavy, top down–driven approaches have been shown to be less effective in the long run than a managed, more gradual transformation. When a large industrial player first attempted to implement secure enterprise architecture, it used a single security point. But that approach led to bottlenecks in performance and system delays. As a result, the company changed its approach and instead tackled changes one process at a time. At one point, it even invited the "white hat" hacker community to partner with it and create a hack-resistant architecture. When choosing where to focus, the company began by securing the most important and technically advanced areas first and worked outward from there.

Encouraging adoption. Companies should embed a business-driven secure architecture into the institutional culture to ensure that it is actively adopted throughout the organization. Companies should offer targeted, role-based training and continuing education for employees at all levels. Education should be based on business terms and easy-to-understand principles and protocols. To foster a security culture, taking educational courses should become part of individual target agreements from the shop-floor to the top-management level.

• • •

Companies are facing a growing array of cyberthreats. Yet heavy investment in building walls can impede functionality and paradoxically lead to new vulnerabilities. Instead, an approach aligned with the business strategy and supported by both IT and business leaders is far more effective. This approach proceeds gradually toward a flexible and scalable target state to serve the company's business priorities as they grow and change.

[1]Oliver Bossert, Chris Ip, and Jürgen Laartz, "A two-speed IT architecture for the digital enterprise," *McKinsey on Business Technology*, December 2014, mckinsey.com.

Oliver Bossert is a senior expert in McKinsey's Frankfurt office, **Wolf Richter** is a principal in the Berlin office, and **Allen Weinberg** is a director in the New York office.