CHAPTER 7

Simplify and Rationalize IT and Security

What you cannot manage, you cannot secure, and a control baseline can't be fully or efficiently implemented across a chaotic IT environment. Although CISOs, or other security leaders, don't own the IT strategy, they have an interest in making it as simple and well defined as possible.

Too many IT environments are aging and dysfunctional. Cloud computing and modern development practices promise transformation to the powerful, seamless IT systems digital businesses need, but often just disrupt, disappoint, and add to the complexity. Amid these challenges, the security leadership needs to be able to reference an up-to-date, approved IT strategy.

To support their organizations' digital transformation initiatives (aka "digital initiatives"), IT organizations must consolidate, simplify, and modernize the infrastructure hosting core business applications. They must rationalize application portfolios. To catch the cloud computing wave, IT and security must change the way they operate from "IT-as-provider" to "IT-as-broker" by excelling at third-party risk management and hybrid cloud monitoring or management. Cloud-enabling processes such as DevOps can take on characteristics of DevSecOps, and Agile of Disciplined Agile, while still enabling rapid innovation.

First the IT and digital innovation, and then the cybersecurity function, must create a strategy that optimizes business agility, operational efficiency, cost-effectiveness, and risk reduction. Although security leaders can't drive the IT or digital strategy on their own, they can request, encourage, and contribute to its development.

Where good practices are lacking, security leaders can advocate for them and implement those that they can as part of ongoing security projects or changes. Security leaders can showcase good practices such as tiered risk assessments, third-party risk

D. Blum, *Rational Cybersecurity for Business*, https://doi.org/10.1007/978-1-4842-5952-8_7

assessments, DevSecOps, and security service catalogs. In many cases, security leaders can leverage their inherently cross-functional role to help promote an effective IT strategy.

This chapter provides guidance on how to

- Address common challenges
- Help develop a strategy to consolidate and simplify IT
- Learn from digital initiatives
- Provide security for a governed multicloud environment
- Upgrade IT operations with DevSecOps and Disciplined Agile

7.1 Address Common Challenges

IT and security organizations often share a common challenge described in Chapter 4's Section "Business Units at Odds with IT and Security." Many organizations' internal IT infrastructures are aging and dysfunctional, losing adoption to cloud-based deployments or digital innovation functions outside the IT chain of command. The drift in larger organizations is toward decentralization as the pace of change in IT accelerates and business units take advantage of cloud services. And yet all too often, digital transformation projects or cloud initiatives end up underdelivering and adding to the complexity of the overall IT environment. The security function gets caught in the middle, charged with protecting a mess not of its own making. Resistance seems futile when security lacks input to the IT or digital strategy or when no strategy is in place.

7.1.1 IT Out of Alignment with Digital Business Initiatives

Is it "IT" or is it "Digital?" Most businesses in 2020 have launched some type of digital transformation project, stood up Digital Innovation Lab(s) at the enterprise or line of business (LOB) level, or even gone so far as to appoint a Chief Digital Officer. This sort of development could be a good thing… or not. Done poorly, competing digital initiatives may cause rival fiefdoms to emerge without uplifting core IT environments.

Shadow IT is an explosion of cloud computing adoption for business use by employees and workgroups with no centralized IT organization involvement. Whereas digital innovation initiatives may be seen as strategic, shadow IT deployments tend to be

more tactical. Between shadow IT and digital initiatives not aligned with IT, it becomes hard to even talk about the IT environment, especially in large organizations. One could ask whether the "IT environment" means *all* the business's IT capabilities regardless of who runs them or just the centrally managed part of IT?

I'll use the term "overall IT environment" inclusively of all IT or digital systems whether they're run by central IT, an LOB, or a CSP. In my experience, even in larger organizations, there's usually one security function nominally responsible for defending or at least overseeing the defense of the whole IT environment. The good news is that, managed correctly, digital initiatives (including shadow IT) can sometimes accelerate the development of digital business capabilities available to all LOBs.

7.1.2 Complexity as the Enemy of Security

Too many IT environments are highly complex, riven into silos, and replete with duplicate capabilities and internal support organizations that become increasingly difficult to sustain. This can happen for the following reasons:

- We (the IT organization) inherit an IT environment that grew organically, not one built and maintained from an architectural blueprint.
- We undertook project after project from a tactical perspective. Projects were underfunded or under-resourced. Project contractors or on-staff developers and engineers failed to provide transfer of knowledge for long-term operations or maintenance. Documentation wasn't created or maintained.
- Our technical debt – or the cost of reworking systems that we still need but find increasingly unfit for purpose – is out of control.
- Different business units, or workgroups, never aligned on a common architecture and portfolio of shared services. They went out on their own to build, buy, or subscribe to YETAs (yet another application(s)) of the same type we already had.

"At the end of a decade or two, IT departments across the business have become curators of IT museums. Old, or suboptimal tools (like a custom financial loan management platform built on Microsoft SharePoint, or many disjointed SAP Enterprise Resource Planning (ERP) modules) have been woven deeply into the business process. They are hard to replace. Dozens of satellite applications, such as customer relationship management (CRM) or business analytics, have been bolted haphazardly on to the tangled mess."

Anonymous Client

Then a new IT opportunity comes along. The "revolutionary" capability or application has an exciting name or buzzword. The business launches a new project driven from a digital innovation team or even from EA. "This is going to change everything, enable the business, reduce costs and risks!" Only it doesn't. Technical debt isn't easy to repay.

Security leaders get caught in the middle, responsible for securing a tangled mess that is not of their making. The more complex an IT system or application is, and the more richly it is integrated into the fabric, the harder it is to secure it. Assurance, or being sure, that something is secure requires threat modeling all the ways it can be attacked and verifying that controls – such as error checking, malware scanning, or configuration hardening – are in place and operating to cover all important attack vectors. Logging services, software updating must be added. A limited budget for assurance and control can run dry amid endless permutations.

The good news is that the security leaders can influence the business toward reducing complexity and following good practices. But security leaders must get themselves positioned correctly in the organization to help drive a coherent IT and security strategy.

7.1.3 New DevOps or Agile Models Fielded Without Security Provisions

Digital businesses, software suppliers, and cloud service providers (CSPs) alike are driven by the market to do more with less and to do it faster. Agile project management can speed release cadences and, in some cases, make service providers more responsive to end customer needs. DevOps models can reduce the number of staff needed to run IT systems as well as streamline the release process.

DevOps is a style of IT operations in which the same team that performs development also performs operations, generally through automated processes. DevOps has become popular due to cloud computing and agile development models in which new capabilities are frequently developed in 2-week sprints, and functionality is released to production continuously. However, DevOps can create security issues if there isn't a separation of duty between development, test, and production operations roles.

"Many organizations are advancing into the DevOps culture but not addressing security in the process. IT and security managers must be prepared to deal with the cultural and technical challenges of defining DevSecOps responsibilities clearly and apportioning them to development and security staff. An additional challenge is that the security environment can be quite dynamic. How can the DevSecOps practices move fast when there's a lot of technical debt?"

David Cross, Senior Vice President, Chief Security Officer at Oracle SaaS Cloud

---

Engaging developers requires a different approach in the (modern) development environment, where agile development models have supplanted the waterfall development models that once ruled the roost. Waterfall software development models[1] – which are heavy on documentation, reviews, and approvals – are favorable for assurance. However, in the digital business environment, most development teams have moved to agile development models[2] that emphasize early delivery, continual adaptation or improvement, and rapid or flexible response to change.

Agile development has become a popular method for creating software, and some businesses even use agile principles or agile project management outside the software development area. However, in some cases agile process has become an excuse for no process at all. It is common to find development teams that don't perform or document up front systems requirements analysis. It can be difficult for security teams to engage development when there is no process to inject security into and no documentation against which to perform security reviews.

[1] "Waterfall Model," Wikipedia, accessed at https://en.wikipedia.org/wiki/Waterfall_model

[2] "Agile Software Development," Wikipedia, accessed at https://en.wikipedia.org/wiki/Agile_software_development

Fortunately, some aspects of both agile and DevOps models can be positive for security, as I'll describe in the section "Upgrade IT Operations with DevSecOps and Disciplined Agile."

7.2 Help Develop a Strategy to Consolidate and Simplify IT

The preceding challenges paint a troubled picture of "macro-complexity" (too many types and instances of systems and applications) and "micro-complexity" (systems integrated in complex or custom ways that aren't well managed or documented). What can CISOs or other security leaders who don't control the IT strategy do? As it turns out – a lot! Start with the following objectives that should be part of any IT strategy:

- Understand how to reduce macro-complexity by consolidating or rationalizing core enterprise applications.
- Understand how to consolidate core infrastructure and security platforms.
- Understand how to simplify micro-complexity by adopting consistent management practices for the IT environment.
- Discern the IT strategy and align the security road map to it.

Take opportunities to position security as a coordinating function, at least informally. Implementing many of these practices is IT's job, but the security function is heavily involved and will live or die based on the outcomes. It pays to understand typical IT strategy objectives and the good practices that can lead to accomplishing the strategy. While doing the security work they have to do within IT anyway, security leaders can align or coordinate with IT, digital, risk, or finance teams already following practices that will support an effective IT strategy.

7-1

Leverage the inherently cross-functional roles security is naturally asked to perform – as policy establisher, access gatekeeper, and security service enabler – to help improve the IT or digital architecture and strategy.

7.2.1 Understand How to Reduce Macro-Complexity by Consolidating or Rationalizing Enterprise Applications

The IT or enterprise architecture (EA) function leads and staffs application rationalization projects, not security. However, security leaders should understand the process and support it in the interests of enabling an IT strategy to help set security priorities, support security objectives, and simplify the IT security environment. So as to be able to talk intelligently on these topics during meetings that shape the IT strategy, let's consider the following brief explanation of application consolidation and rationalization.

Every business has its core operating and administration functions, such as

- Product or service development, manufacturing, or extraction
- Logistics, communications, transportation, or delivery
- Sales and marketing
- Product or service delivery, customer support, accounting, etc.

There may be more than one core application instance, for example, a retail and manufacturing conglomerate has multiple "cash cow" product lines; a national government has multiple departments.

IT organizations can identify core functions of the business and map them to core applications as follows:

- For each line of business, name the core operating functions and list the applications that support them.
- Next, identify the administration functions – such as HR, accounting, facilities, legal – that support each line of business and list the applications that support them.

You don't have to generate a complete list of *all* the applications that enhance or support the core applications; that comes later with the application portfolio exercise. Core applications are just the main applications.

Rearchitect or Rationalize Core Applications

In studying the core functions of the business, one often finds multiple core application vendors used for multiple lines of business, for example, both SAP and Oracle for general administration and Microsoft, IBM, and some open source tools

for product development in the same area. Ideally, there could be one and only one core application suite for each core function. Rationalizing applications is the process of phasing out applications that do the same thing or at least specifying which is the enterprise standard and requiring LOBs to justify using a different solution.

One may also discover an aging core application or perhaps an old version of the vendor's product. Whenever possible, core applications should be based on modern architectures using a recent version of the product or service. IT or development organizations can also refactor core applications by eliminating now-unnecessary modules, replacing ones that are easy to replace, and wrapping others with APIs. Eventually the code in the wrapped modules can be pulled out into microservices or itself replaced. Often, application-specific security modules can also be refactored to use general-purpose security products (i.e., for encryption or identity management functions).

Also, per the following cybersecurity-business alignment key, some specific security-related controls may benefit from competent application portfolio management.

7-2

Coordinate the asset inventory control and asset risk profiling implementation, timing, and data models with those of IT- or EA-led application consolidation and rationalization efforts.

7.2.2 Understand How to Consolidate Core Infrastructure and Security Platforms

IT or EA should develop an IT strategy for consolidating infrastructure platforms as well as enterprise applications. Security controls must be implemented in the infrastructure using a combination of native platform capabilities and multiplatform (or hybrid cloud) integration patterns. Simplifying infrastructure security systems (especially identity and access management (IAM) and logging) yields major benefits to security team workloads and accuracy.

Infrastructure Platform Background

A core infrastructure platform provides the set of hardware or software compute, storage, and network capabilities needed to support one or more business applications. It includes physical or virtual servers and containers, operating systems (OSes), network routers, and storage facilities.

Examples of infrastructure platforms include public cloud infrastructure-as-a-service (IaaS) solutions – such as Amazon Web Services (AWS), Google Cloud Platform, and Microsoft Azure – as well as private cloud, premise-based solutions based on VMware or virtual data center solutions. Vendors such as Cisco, Juniper, and EMC provide the network and storage capabilities for private clouds and in some cases in partnership with public cloud suppliers.

Security in the IT Strategy for Infrastructure Platforms

The IT strategy should seek to minimize the number of infrastructure platforms. Otherwise, the more platforms and the more integration patterns are required, the more complex the control baseline(s) becomes along with all other aspects of IT management and security.

Often, strategists advocate moving infrastructure to public IaaS systems so as to simplify IT. However, although IaaS offloads operations tasks such as data center and server hardware management, it still leaves the customer to manage operating systems, network zoning, performance, availability, backups, and more. Any IaaS that isn't required to support a core business application is fair game for consolidation. When rationalizing or rearchitecting core applications, businesses should consider the infrastructure consolidation too. One option is to source new versions of core applications from a software-as-a-service (SaaS) solution. SaaS completely offloads IaaS requirements from the customer. Most software vendors are shifting their strategic development priority into a cloud offering such as Microsoft Office 365, Oracle Data Cloud, and SAP HANA.

IaaS or private cloud solutions remain the only choice, however, when a business's core applications are either developed in-house or must be heavily customized beyond the limits of vendors' SaaS solution flexibility. Even then, platform-as-a-service (PaaS) or "serverless" deployment options on IaaS may be an option. Typically, an in-house private cloud infrastructure and one or at most two public cloud IaaS infrastructure platforms can satisfy most business infrastructure platform needs.

Each infrastructure platform requires a skilled team to operate and maintain it, and any security controls must be operationalized for it. For example, a compliance regulation or the business's own security policy might require encryption of sensitive data-at-rest in all platforms. Encryption key management could then be implemented using platform-native capabilities (such as Amazon Key Management Services (KMS)) or a third-party capability (such as the Thales/SafeNet virtual key management servers

running in AWS). If the business also used VMware in its private cloud, it would have to implement encryption key management there as well. Potentially, elements of the same third-party encryption key management capability can be used across the hybrid cloud of multiple infrastructure platforms.

7-3

Work with IT infrastructure platform teams to develop a menu of reusable native or hybrid cloud capable security controls. Communicate security recommendations to IT teams and application developers for using the preferred (strategic) controls and/or guidance and decision trees for control selection.

7.2.3 Understand How to Simplify Micro-Complexity by Adopting Consistent Management Practices for the IT Environment

Many core IT systems are highly configurable and complex to deploy – think Windows Active Directory domains with interforest trusts or SAP and Oracle ERP suites each integrated with 20, 50, or even more satellite applications for development, collaboration, or analytics. One such core system isn't even the whole IT environment, but if you draw out all its inputs, outputs, services, and dependencies, it can sometimes look like the proverbial tangled mess.

Fortunately, core systems setup need not be complex and obtuse. Solution engineers can simplify the micro-complexity of the larger core systems through standard architecture patterns for identity, security, network, storage, monitoring, data models, and business continuity. By tackling macro-complexity through consolidation and micro-complexity through good deployment practices, IT can reduce or avoid technical debt.

Since much of the micro-complexity comes *from* security, the security team has a natural mandate and many opportunities to help reduce it. To do so requires close engagement and collaboration with IT.

7.2.4 Discern the IT Strategy and Align the Security Road Map to It

Security leaders have a stake in simplifying and rationalizing IT. Although they can't drive the IT strategy on their own, they can request, encourage, and contribute to its development. Without an IT architecture and strategy in a business of any complexity, there can be just too many moving parts to protect.

Security leaders must look through the lens of risk first. Even if highly sensitive data is mired in a legacy system one hopes to replace, it is still a protection priority. But the IT strategy should be the secondary prioritization lens to help pick investments in controls for strategic and thus future-proofed IT systems.

If an up-to-date, approved IT strategy is available, security leaders can align the security strategy, architecture, and road map cleanly and completely to it. Tying security control solution architectures into the known quantity of an IT strategy and road map does wonders to clarify security priorities from the technical control perspective.

If no strategy is published, try to determine the de facto IT strategy by understanding the assumptions and road maps of IT leaders and major LOBs. Work with IT leaders, EA, digital initiative leaders, and risk management functions to resolve open issues or answered questions on strategic IT or digital targets to secure. The goal is to determine which applications, infrastructure platforms, and integration patterns are core to the business and are considered strategic priorities by the leadership. Align security priorities for capability deployment and improvement to those. Ensure that any gaps in the business's understanding of the IT strategy get reflected as gaps in the security road map as well.

Of course, trying to fill a gap in IT strategy isn't always easy. Security leaders can find themselves in an awkward position. IT leaders may not be ready or interested.

"Most organizations are barreling along in one direction 'driven by culture,' and you won't succeed by standing out in front and telling folks they're going the wrong way. If you want to steer in a new direction you first need to find ways to influence the drivers by identifying shared interests and finding their pain."

Jack Jones, Chairman of FAIR Institute

Work collaboratively on common priorities or pain points. Security teams should always be able to identify opportunities to work with IT on shared priorities because often much of the micro-complexity of IT comes from "kludgy" security bolted on in a haphazard manner. Refactoring security services such as monitoring, patching, and access management to use loosely coupled, API-enabled components can reduce technical debt and set the stage for further modernization.

Collaborate with IT on developing security controls. Every control from cutting-edge new DevSecOps capabilities to traditional patch management affects IT, by its nature, and is a natural meeting ground for IT and security staff to work together. Pick at least two different control groups from different categories in the control baseline (e.g., asset inventory, secure system configuration, or logging and log review) for joint projects with IT. Involve IT staff in the design, follow a repeatable project methodology, and document the results such that the project can showcase security and IT working together.

7.2.5 Take Opportunities to Position Security as a Coordinating Function

It's not uncommon for organizations to have a decentralized IT environment where business units control much of the IT budget and staff. Security can often serve as a coordinating function between IT, LOBs, and corporate administration groups. Working on an informal basis across these groups, security professionals tend to have a useful cross-functional view. It isn't always realistic to formalize a coordinating role for security leaders, but some of them thrive on it.

ENGAGED SECURITY LEADERSHIP STORIES

"I work with a Security Business Liaison Committee run by the CISO to manage the timing and impact of technology and policy changes at the bank. The committee has sub-groups for executives, mid-level managers, and technical coordination. As a security strategist, I add value to IT and the business strategy by helping to solve multi-disciplinary problems that none of the groups could solve by themselves."

Randall Gamby, Vice President, Manager Security Strategy at U.S. Bank

"We have an EDGE team ('Everyone Digs Governance Eventually') for security, compliance, HR, legal, Growth, Finance, and all the business units. Through EDGE, we facilitate solutions to 'sticky yucky' business problems requiring multiple stakeholders to resolve. We've tackled everything from how to ship medical data extracts to partners in a secure and compliant manner, to vendor risk management, to securing merger and acquisition processes. I've spent a lot of time building up my Associate VPs to help me engage the business."

Joey Johnson, CISO, Premise Health (ISE Southeast Executive Award Winner 2017)

7.3 Learn from Digital Initiatives

The security team can be a fast learner that adopts good practices from formal or informal digital initiatives and pockets of innovation in the organization or even externally to it. Security leaders should maintain contact wherever possible with groups outside IT that are responsible for digital initiatives. At a minimum, keeping an open channel provides the opportunity to familiarize such teams with current security service catalog options, decision trees, or other implementation aids used for similar efforts in the past.

Recognize that as a digital business, parts of the IT and the application environment may be in a state of continuous transformation and disruption. Be open to the possibility that the digital team(s) is uncovering new or unique use cases and requirements for which IT and security leaders do not yet have a fit-for-purpose solution. Be prepared to partner with the digital team and learn from it, potentially assisting its efforts and bringing new skills, knowledge, and capabilities back into the security offering and/or strategy.

7.4 Provide Security for a Governed Multicloud Environment

To succeed, the IT and security leadership must make capabilities available to business units in an easy-to-consume, agile manner. Gone are the days when business units would live with lengthy IT schedules for delivering new capabilities or changes; today they can quickly put any one of hundreds of SaaS offerings on a credit card or hire a few

developers to build a custom solution on an IaaS platform such as AWS or Azure. Many businesses have adopted a "cloud-first" IT strategy where IT or LOBs deploying premise-based solutions must justify why this approach is superior to cloud-based options.

With some businesses even opting for a "cloud-only" IT strategy, one might ask is there even a need for an IT department? I think the answer is yes because the business needs IT expertise to deliver on the cloud's promise of lowered cost and increased agility as well as to manage security and risk. However, IT and security groups must prove this point to the business through action.

7.4.1 Identify the Risk of Shadow IT

Shadow IT can lead to unintended and undesirable security risks, compliance concerns, and hidden costs. According to the Oracle and KPMG Cloud Threat Report 2019,[3] 92% of 450 IT and security respondents were concerned about shadow IT; many of the respondents also found that policies against the use of unauthorized services were routinely flouted and had led to unauthorized use of data, introduction of malware, and other issues.

On the other hand, Entrust Datacard's report, "The Upside of Shadow IT: Productivity Meets IT Security,"[4] found that 77% of 1000 respondents believed shadow IT can make businesses more competitive and that efforts to eradicate it through cumbersome approval processes could actually drive business or IT users even farther into the shadows and compound the problem.

Rather than thinking of these as dueling reports, we can see them meeting in the middle on the need for a governed enterprise multicloud offering. Facing a clear and present danger, businesses will often empower security to develop a strategy for controlling shadow IT. When that happens, security leaders should resist the temptation to come down too hard on shadow IT offending LOBs with draconian policies. Instead they can engage the business leaders and help them understand risks and accountabilities.

[3] "Oracle and KPMG Cloud Threat Report 2019," Oracle and KPMG, April 2019, accessed at www.oracle.com/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf

[4] "The Upside of Shadow IT: Productivity Meets IT Security," Entrust Datacard, October 2019, accessed at www.entrustdatacard.com/pages/shadow-it

7-4

Work with forward-thinking IT leaders seeking to establish IT as a broker in the cloud environment.

With the security team's support and a business mandate, IT should be able to resolve the shadow IT conundrum, as also discussed in my article, "Shadow IT: Cultivating the Garden,[5]" and in the following section.

7.4.2 Align with the Evolution from IT-as-Provider to IT-as-Broker

A cloud-only or cloud-first approach is a game changer for the IT department. Now it must operate as a broker of cloud services as well as a provider. Businesses can mitigate the risks of shadow IT by having the IT and security organizations develop a service catalog of shared capabilities – both cloud-sourced and from in-house. IT can also help business units find the best cloud solutions for their needs and help the enterprise by curating all business unit requirements and satisfying them through the fewest possible number of reusable, flexible, and scalable solutions.

The first step is for IT to marshal cloud computing expertise from within its ranks to create one or more Cloud Architect and Cloud Security Architect positions with performance objectives to support LOBs and digital initiatives. Then open a communication flow such that

- IT Cloud Architects and Cloud Security Architects become familiar with cloud developments within the business and provide periodic internal briefings on IT projects, LOB projects, industry technology developments, and the state of the market.
- IT and security communicate the IT strategy, service catalogs, and road maps incorporating shared cloud services to the business.

[5]"Shadow IT: Cultivating the Garden," Dan Blum, November 2019, accessed at https://security-architect.com/shadow-cultivating-garden/

- LOBs engage IT and security from the beginning of capability sourcing decision processes.
- Business, IT, and security staff establish informal working groups (aka centers of excellence) to share knowledge of cloud applications and infrastructure platforms.

The cloud access security broker (CASB) is an example of a security tool that both controls and enables cloud users. By providing single sign-on (SSO) to cloud services, the CASB improves ease of use, user authentication, and user account management assurance. The CASB can also support financial controls by limiting cloud access for sanctioned services to users with centrally authorized accounts. Licenses for unauthorized users could be reclaimed.

Additional cloud-enabling services provided or supported by centralized IT groups could include consulting, implementation, DevSecOps, monitoring, IAM enablement, and more. As we unpack the topic of business-enabling technology services and topics, security comes into increasing focus and with it opportunities to encourage and influence a modern IT strategy and service delivery model.

7.4.3 Manage Cloud Risk Through the Third-Party Management Program

In practice, there is a natural tension between consolidating forces in IT and decentralizing forces in the LOBs and development organizations. How the business manages third-party relationships (or doesn't manage them) can end up becoming a battleground.

7-5

Work with third-party management to develop a portfolio process for managing the risk and utility of third parties.

Developing a tiered risk assessment process (see Chapter 5, section "Implement Tiered Risk Assessment") for third parties is not so difficult for smaller business with security staff ready to do their research. Larger business with multiple LOBs and a need for hundreds of third parties should consider obtaining a third-party risk management tool, such as BitSight, ProcessUnity, or Security Scorecard.

A BROKERAGE'S THIRD-PARTY RISK MANAGEMENT STORY

At a recent conference, BitSight copresented a case study of a third-party management process with one of its financial services brokerage clients.

BitSight is a Vendor Relationship Management (VRM) vendor that provides a security rating service for third-party vendors' and CSPs' security postures. At the conference the brokerage described how it used the technology to develop a successful process.

"Management liked how we required vendors with high risks to have high scores," said the speaker. "We operate similarly to a mortgage lender's loan pre-qualification service. Suppose a business unit brought us proposal to use a vendor with a low score. Using BitSight's database during a 30-minute meeting with the internal customer, we could explain the issues with the vendor and propose some alternatives.

"In general, we don't focus much on the low risk use cases, but we can really help with the medium-risk scenarios. For those, we have made the assessment and implementation into parallel processes. This lets us pick our battles. In high risk scenarios (e.g., ones requiring the vendor host our customers' personal data) we got the LOBs to agree to follow a policy of no implementation until an assessment using questionnaires and site visit is complete. The database tool also helps us determine what areas to dive into.

Bottom line – we've gone from taking 17 weeks to as little as 1 day for pre-qualification and have even been able to reduce the high risk review process to less than 8 weeks."

7.4.4 Collaborate with IT on Operationalizing Shared Security Responsibilities

Security and IT management across the industry are adapting to the "hybrid IT" model. As the business rationalizes core systems, some capabilities move to the cloud. These capabilities need to be deployed and operated using a shared responsibility model with the CSP as well as central IT and/or LOB-level groups. Many IT teams are not as experienced working in the cloud model, and shared responsibility arrangements tend to be addressed as one-offs in an ad hoc manner.

To simplify and rationalize the hybrid IT environment, businesses should systematize a shared responsibility model in technology processes for onboarding new CSPs or new cloud services, change management for existing services, and service

decommissioning. The process can engage appropriate groups from the business (i.e., third-party management for contracts, IT and security for risk assessments, and IT and the CSP for operations protocols). See Chapter 6, section "Apply a Shared Responsibility Model to the Control Baseline" for more information.

7.4.5 Include Security Services in the IT Service Catalog

The concept of a service catalog becomes increasingly compelling with hybrid IT and IT broker/provider operating models. The catalog is a documented set of IT service offerings that provides a unified view of IT capabilities independently of where they're sourced from, how they're operated, and who maintains them. Thus, the service catalog can broker both IT and CSP-provided services to internal customers. All that is required for a capability to be on the catalog is that it follows whatever contracts, service-level agreements (SLA), or cost model standards the catalog defines.

- **Contracts:** Usually internal agreements, but sometimes legal agreements, on how the service will be consumed or provided
- **SLAs:** IT or service provider commitments to uptime, support response time, or other performance metrics in operating the service
- **Cost model:** Chargeback or showback processes that enable the business to assess internal cost structures and how resources are allocated

Most cybersecurity capabilities and activities can be factored into IT service offerings – some to be exposed to the business and others measured only within internal IT processes. A security capability or activity can be

- **Provided as a stand-alone IT service catalog item:** For example, a business could offer both standard and enhanced email hygiene services to business units with different service descriptions and lower or higher SLAs and costs. The standard service could provide email anti-spam and malware scanning as well as anti-phishing awareness training. The enhanced service could add deep email anti-malware sandbox analysis and enhanced services for signed or encrypted email delivery.

- **Packaged into the IT service catalog and exposed to business stakeholders.** For example, a Standard Linux Server could be provided as a virtual machine (VM) on a private VMware cloud or on the AWS IaaS. In either case vulnerability management SLAs could specify how often the VM will be scanned and the patching windows.
- **Embedded into the IT service catalog but not exposed:** Certain capabilities such as user entity behavior analysis (UEBA) or security configuration checking could operate on critical systems without an exposed SLA and/or service description.

Notice how closely IT and cybersecurity services can sometimes be interwoven. To achieve higher maturity, the security function should be providing service catalog information. In doing so, it can either align with an existing IT service catalog process or engage with IT to develop one.

7.5 Upgrade IT Operations with DevSecOps and Disciplined Agile

DevOps benefits may come at the expense of losing separation of duty between staff roles and may even undermine the separation of IT development environments from IT production environments. If a fully automated continuous delivery, continuous deployment (CICD) model is adopted, the requirement for handover, or signoff, may be omitted. Fortunately, development teams (motivated to deliver more functionality on schedule) and operations teams (motivated to only deploy stable solutions that run reliably) tend to work well together for availability objectives. But what about privacy, confidentiality, safety, or integrity concerns?

7.5.1 Use Risk-Informed DevSecOps Practices

Although DevOps poses a challenge for cybersecurity, it's also an opportunity. Some of the DevOps principles – automation, systems thinking, continuous improvement, transparency, and shortened feedback loops – can be positive for assurance.

DevSecOps is the name for the practice of adding assurance into DevOps processes. As shown in Figure 7-1, it affects the timing, impact, and scope of security steps in the DevOps process.

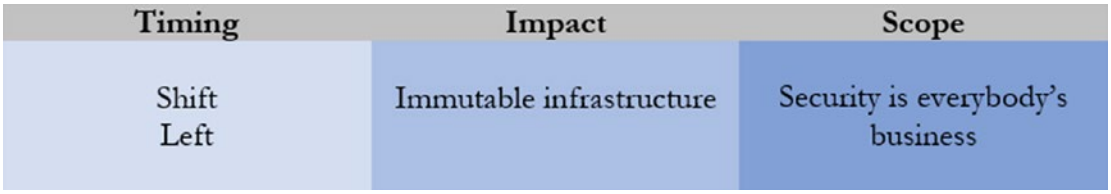

Figure 7-1. *DevSecOps Benefits*

- **Timing:** DevSecOps "shifts left" the security assurance steps in DevOps release process, enabling IT to build security practices in at the beginning of projects rather than bolting it on at the back end.
- **Impact:** Automated deployment, aka "infrastructure as code," eliminates one big vulnerability: the need for system administrators to get remote access into production server farms and applications to reconfigure systems or fix bugs. The "immutable infrastructure" is never reconfigured or patched directly in production. Instead, it is updated periodically from the latest stable development or QA version. Malware has fewer ways to infect immutable infrastructure and would be more easily detected.
- **Scope:** Not only are security steps automated, or semiautomated, into the development and release processes, they're also defined in a simplified manner so that the developers themselves can perform them with appropriate security training and review. DevSecOps can be a force multiplier for the security team.

7-6

Empower developers to easily perform security-related tasks (DevSecOps) as part of their normal workflow and/or cross-fertilize security staff or expertise into the development organization.

To start a DevSecOps initiative, security teams can engage developer communities using a combination of these approaches:

- **Work alongside pilot projects to instrument security steps:** Security staff can be temporarily embedded within key development organizations to build security instrumentation into the release process. The goal should be to configure development pipeline tools to invoke security steps in an automated manner to minimize the developer impact of the extra work on successive releases. Work with developers to capture the learnings on how to analyze reports from security tools (such as static and dynamic code testing) on their systems, simplify the process of fixing problems, and develop training curricula for others based on the pilot project experience.
- **Designate security champions:** Matrix key software architects to the security organization. Identify persons on the developer teams who are willing to take on the opportunity for an expanded role via a security championship program. Provide executive support and other incentives to encourage participation.

TECH COMPANY'S SECURITY CHAMPIONSHIP STORY[6]

"We were able to improve our vulnerability metrics and expand the extended security team from 15 to 40 participants without adding security headcount. We did this using business engagement, collaboratively developed metrics, and a security championship program that followed three principles: Inclusion, Transparency, and Governance.

We engaged security champion volunteers on every major team. With the approval of their VP each security champion dedicated 15% of their time for hands-on security-related work in their area. In return they got recognition and reimbursement for training courses through which they earned paid security certifications.

[6]"Democratizing Security: A Story of Security Decentralization," Harshil Parikh, March 2019, accessed at https://published-prd.lanyonevents.com/published/rsaus19/sessionsFiles/13748/HUM-W03-Democratizing-Security-A-Story-of-Security-Decentralization.pdf

We also worked with business leaders to build consensus on security metrics and ways to improve them. We developed tools to show the measurements to leadership frequently using positive messaging (not a wall of shame).”

Harshil Parikh, Security Leader, Medallia, Inc.

Cover the Full Software Development Life Cycle (SDLC) Process

The scope of DevSecOps may cover anything from lightly customized commercial software and services integrated together in test and production environments to large, custom-coded applications. As we discussed in Chapter 6, software security then becomes a critical part of the control baseline and typically involves DevOps teams adhering to enterprise SDLC standards.

Figure 7-2 details a sample DevSecOps-inspired development and release process diagram. Security steps track each stage of the process and can be highly automated. Training for new staff on the SDLC and its embedded security steps can be delivered just in time or at the beginning of projects. As developers create and unit-test software modules, they perform code scans or static security tests. Once developers integrate code into larger modules, dynamic application security tests attempt exploits against the runtime interfaces.

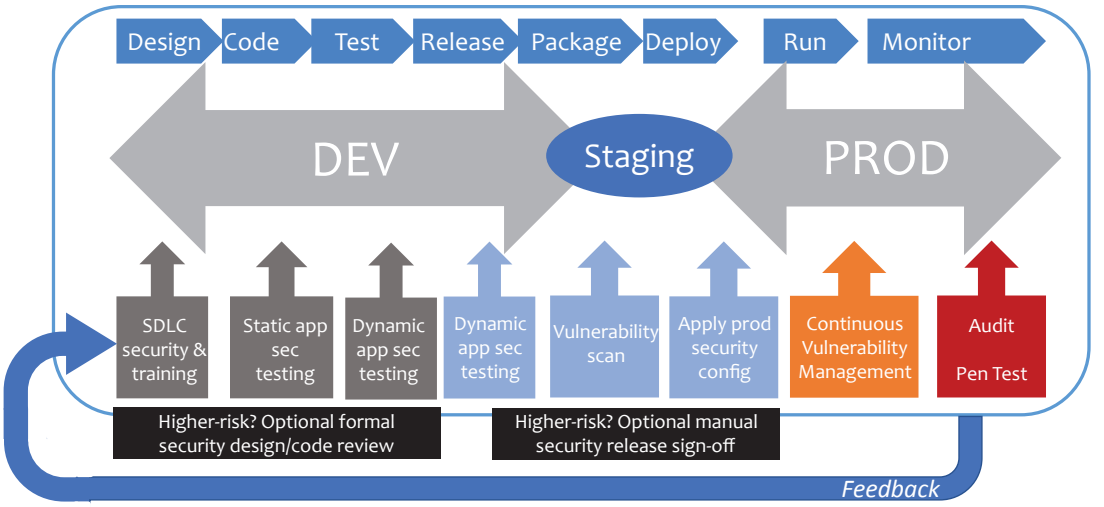

Figure 7-2. *Sample DevSecOps Process Diagram*

As DevOps teams prepare the product for production, they perform vulnerability scans and apply production security configuration. In production, continuous vulnerability scans and patch updates begin, the security team does periodic penetration tests, and security operations or internal audit monitor events or logs.

Security teams can also consider performing formal security design or code reviews for higher-risk projects, as well as requiring manual security release signoff before promoting changes to production. Note, however, that formal reviews are expensive and require specialized security expertise. They are typically reserved for the most sensitive modules (i.e., cryptographic processors, automated teller machine (ATM) user interfaces) in high-risk systems. Another alternative is to provide guidance or training to help senior developers that perform design reviews for integrated systems to look for specific kinds of security issues.

Finally, security and development organizations can collect continuous feedback from the DevSecOps process, including both automated metrics, such as the results of the security tests, and qualitative lessons learned or suggestions to improve the SDLC process. Track such feedback in an issue management system, such as Jira or ServiceNow.

7.5.2 Embrace the Disciplined Agile Approach

In the "Address Common Challenges" section, we noted that, sometimes, the "agile" methodology is used in practice as an excuse for no process at all. Agile's silver lining, however, is the notion that agile development teams, or "squads," should have end-to-end accountability for delivering their minimum viable product. This can and should be construed to include mitigating risk. If one of our goals for Rational Cybersecurity is to "make security everybody's business," what's not to like about a methodology that emphasizes accountability?

Enter the Disciplined Agile Delivery (DAD) model.[7] It adapts agile methodologies, such as Scrum and Kanban, to make them more suitable for larger projects requiring cross-functional coordination or higher-risk projects requiring assurance and oversight.

[7]"Disciplined Agile Delivery," Wikipedia, accessed at https://en.wikipedia.org/wiki/Disciplined_agile_delivery

DAD enables agile teams to continue using their agile methodology of choice while extending it to support coordination and assurance at project inception, construction, and transition stages.

- **DAD inception:** Kicks off the typical series of agile work streams broken up into two-week "sprints" with a "Sprint 0" inception stage. Sprint 0 has just enough up-front planning to solidify the vision for the project or application as well as the scope of the effort, overall data model, and technical architecture. Also, the inception stage can identify the expected risks, testing strategy, and whether the application will be reused by others.
- **DAD construction:** Actual DAD development proceeds similarly to Scrum or Kanban's; however, teams include an architecture owner role and have the remit to coordinate with colleagues in supporting roles for testing, integration, and project-specific specialties.
- **DAD transition:** Adds sprints as necessary for the DAD team(s) to transition a capability into production. The primary DAD team(s) coordinates with infrastructure, security, operations, and support during the release process.

DevOps and DevSecOps teams can adopt key concepts from DAD for projects that exceed agreed risk thresholds. The security organization can also use DAD for its own security engineering efforts and share knowledge, tools, and lessons learned with development organizations so as to influence DAD's inclusion in the SDLC. DAD procedures and supporting roles can be coordinated with DevSecOps. For example, a project inception stage could specify a test plan with requirements for the manual or automated security steps during development and integration with security tools for functions such as encryption or vulnerability management.

7.6 Call to Action

The core recommendations for security leaders from this chapter are to work with IT on simplifying and rationalizing the IT environment as follows:

- Identify and help solve IT and business leaders' security-related pain points in IT systems.
- Leverage the cross-functional roles security is naturally asked to perform – as policy establisher, access gatekeeper, and security service enabler – to help improve the IT architecture and strategy.
- Prioritize security solutions based on an already written or de facto IT strategy.
- Coordinate work on controls such as asset risk profiling (as part of asset inventory) with application consolidation and rationalization efforts.
- Develop security architecture patterns, recommended solutions, and decision trees to apply controls in core infrastructure platforms.
- Support forward-thinking IT leaders seeking to establish IT-as-broker in the cloud environment and/or finance projects working to put technical debt on the balance sheet.
- Work with third-party management to develop a portfolio process for managing the risk and utility of third parties.
- Include security services in the IT service catalog.
- Cross-fertilize security staff or expertise into development and/or operations organizations to establish risk-informed DevSecOps and Disciplined Agile practices.

Action – Make a quick assessment of the state of the organization's IT security strategy and architecture

Ask yourself the following short set of questions and score the answers in the Success Plan Worksheet's[8] Section 3, Table 3. Base the scoring criteria on whether you would answer most of the questions with a strong "no" (1), a strong "yes" (5), or something in between.

1. Does the business have a simplified and rationalized IT environment?
2. Is there a published, up-to-date IT strategy?
3. Has the security strategy aligned to the IT strategy?
4. Is the business use of a hybrid multicloud environment governed well?
5. Does IT publish a service catalog and are security services included in it?
6. Does the security organization work closely with third-party management to assess risk early in the commercial evaluation process?
7. Is the security organization working with DevOps teams to develop DevSecOps processes?

Action – Define 1–3 improvement objectives for simplifying IT and security
Note improvement objectives in Section 4, Table 8, of the worksheet.
The following are examples of IT and security strategy–related improvement objectives:

- Locate document(s) labeled as an "IT Strategy" or serving that purpose. Provide security organization commentary on them and discuss with the IT stakeholders. Align them with the current security project portfolio or road map as appropriate.
- Help the IT organization operate in the "IT-as-broker" mode by collecting information on cloud-based security services options (e.g., vulnerability scanning, multifactor authentication, etc.) already provided.

[8]"Rational Cybersecurity Success Plan Worksheet," Dan Blum, Security Architects LLC, May 2020, accessed at https://security-architect.com/SuccessPlanWorksheet

- Analyze development tool chains in use and discuss potential DevSecOps solutions with development managers.
- Evaluate the opportunity to set up a Security Championship Program(s) in IT. Discuss the idea with senior IT managers that might support it and/or identify staff members in IT that might be good candidates in championship roles.

Don't limit yourself to these examples. Look for improvement objectives that fit the gaps and priorities you've identified for your business.