Interconnectivity Innovation

In today's business world, few organizations larger than a small enterprise can survive without interconnectivity limited to just email or a website. Even smaller not-for-profit organizations are using tools that provide greater interconnectivity. From an innovation perspective, interconnectivity tools have exploded. Those solutions have caused changes to traditional architecture, such as where data are stored, how networks are structured, and how we apply security. The downstream changes themselves have been products of innovation to address the growing needs of business to interoperate in a more open world while still providing the security and privacy organizations require.

If security and audit teams wait until a particular tool is selected, then those teams are operating in catch-up mode, as the gains provided by those tools are strong drivers for early or immediate adoption.

Collaboration Tools

In recent years, cloud-based collaboration tools have exploded because of the increase in external consulting and outsourcing. Looking beyond product offerings such as Google Docs and Office 365, there are a great number of document and project management tools available. It is important to enumerate some of the risk areas we need to proactively address.

First, if the external agency initiates the use of those resources, it likely retains control of the security and sharing. The organization incurs risk because that external party could inadvertently grant access to those resources. The organization's standard controls for entitlements/authorizations do not examine those resources to detect issues.

The second risk is the content stored. Any time an organization deals with a third party, there is always the risk that data sensitive to the organization are stored on that third party's systems. That could be something as simple as notes in OneNote for a consultant for a current feature on which that person is working. This risk exists even if all the collaboration happens on the organization's controlled systems. The issue with cloud-based collaboration systems is that it is hard for an organization's data loss protection (DLP) systems to be brought to bear. Connections to those collaboration tools are using encrypted over Hypertext Transfer Protocol Secure (HTTPS), so unless the collaboration system does not have safeguards that prevent the standard decryption and inspection method used by web filtering systems, DLP cannot see the sent data. It certainly cannot see things from the third party's side. As a result, there is the possibility that someone will put sensitive data into those collaboration systems that should never have left the organization's control.

A third risk is the ability to recover if data are inadvertently changed or deleted. Different systems have different capabilities. An organization should know what its own recovery capabilities are for the systems within its full control. Even if the organization is using a provider such as Amazon

K. Brian Kelley, CISA, CSPO, MCSE, Security+
Is an author and columnist focusing primarily on Microsoft SQL Server and Windows security. He currently serves as a data architect and an independent infrastructure/security architect concentrating on Active Directory, SQL Server and Windows Server. He has served in a myriad of other positions, including senior database administrator, data warehouse architect, web developer, incident response team lead and project manager. Kelley has spoken at 24 Hours of PASS, IT/Dev Connections, SQLConnections, the TechnoSecurity and Forensics Investigation Conference, the IT GRC Forum, SyntaxCon, and at various SQL Saturdays, Code Camps and user groups.

> WITH A SYSTEM THAT A THIRD PARTY CHOOSES, THERE IS NO GUARANTEE THAT THE SYSTEM WILL MEET THE ORGANIZATION'S RECOVERY REQUIREMENTS.

Web Services (AWS) or Azure, the technical team should be fully aware of what those providers' different offerings have for recovery. With a system that a third party chooses, there is no guarantee that the system will meet the organization's recovery requirements.

A fourth risk is adherence to data retention standards. Whether the system is under the control of a third party or the organization has adopted it quickly because of a push from business, the majority of the time the focus is on authentication/authorization and, just as with recovery, data retention is an afterthought, if it is considered at all.

Data in the Cloud

Speaking of data retention and DLP, we are seeing more data going into cloud systems. Managing and protecting data in the cloud is similar in concept to on-premises systems but may differ greatly in actual implementation. For instance, an organization may follow a particular benchmark or security standard with respect to a product. However, the version of the product hosted by a cloud provider may not allow for some of the settings or controls that the organization can enforce on-premises.

In addition, an organization has to consider how to move data around. When everything is all in one place, whether that be the cloud or on-premises, there typically is not significant cost to moving data around. This is especially true when everything is on-premises. However, in hybrid scenarios, cloud providers often "run the meter" on data transferred. Most of the time, the data you pull out of the cloud are on what the provider bills. However, in some scenarios, it is both directions. Since part of audit's responsibility is providing oversight in how an organization uses its resources, auditors may find themselves reviewing the billing vs. the actual usage and value of the resources being billed. This billing is different than in traditional models, which have the bulk of the cost up front. The advantage of that traditional model is that the possibility of a surprise large bill is low. With consumption-based billing, the norm for the cloud, unexpected increased charges happen too often. For those of us who lived in the cell phone era where you had to keep track of your minutes and watch for roaming charges, it is that same pit-in-your-stomach worry, but now applied to cloud.

Data governance is another area that is harder. For instance, there was a case where the vendor indicated data in flight were encrypted for its cloud-based solution. In reality, the path across the Internet was encrypted because it was a web application and communication was over HTTPS. However, inside the vendor's network, to include when the data were stored, the vendor did not use encryption. Given the nature of the system, it was shocking that the vendor did not encrypt. This is just one aspect of data governance. With data classification, for instance, it is even harder to ensure that the vendor has the proper controls.

More Open Networks

The old network security model is to have an impenetrable boundary between the trusted network and everything else. If the organization has resources that others from outside the organization should access, such as Internet-facing web servers, there are two boundaries. Traffic from an area of lower trust, such as outside the organization, to higher trust—inside the private network—have strict rules. However, traffic in the opposite direction or within the same area, such as all on the private network, often have few rules to restrict traffic in the old model.

With newer solutions, this model is outdated. In fact, it may inhibit the features and advantages that newer innovations seek to deliver. For instance, many of these newer tools are designed to be accessed anywhere, as long as a user has an Internet connection. There is no virtual private network (VPN) connection. There is no brokered access to an internal network. One can simply connect, authenticate and off they go. However, not only does this user have this kind of access, so does everyone else.

Networks need to be more open. This brings a new set of headaches. How do auditors and security professionals ensure that the organization's assets

are properly secured? How do they know if someone is trying to access their resources when outsiders should not be able to do so? For especially sensitive or privileged operations, do practitioners have the ability to set controls such that multifactor authentication (MFA) is used? Can they restrict to a certain region of the world based on Internet Protocol (IP)? Can they determine what the normal usage pattern for a privileged user is and block if the usage is outside of that? What exactly do they need to protect with these options? Which options do practitioners apply and which ones are too much? As auditors and security professionals, there are a great deal of things to consider to protect our organizations.

> "A USER OR SYSTEM DOES NOT AUTOMATICALLY GET TO TALK TO A RESOURCE JUST BECAUSE BOTH ARE ON THE FORMERLY 'TRUSTED' NETWORK."

Beyond Productivity

I have discussed the risk areas in some detail, and one could walk away gloomy about all the challenges before us with increased interconnectivity. Innovations are not limited to productivity. We have made gains in security as well. In evaluating how to protect an organization in the face of increased interconnectivity, we have come to realize that our old network security model is an artifact of the past. I have heard it referred to as the M&M security model after the popular candy: a hard outer layer with a squishy inside. Once you make it past that hard outer layer, traversing inside the private network is easy. So, all I have to do is find a way inside. With options such as phishing attacks, default configurations, and security awareness failures, an adversary has a host of options to break through.

The real problem, then, is that the squishy inside is squishy. We know adversaries are going to get inside. It is not if, but when. Moreover, we still have insider threats from malicious actors within our own organization. We spend a great deal of time talking about external enemies, but the insider threat has not gone away. This has led to concepts and efforts such as the zero trust network security model and ways to implement such a model, such as with software-defined networking (SDN).

Now security practitioners should segment resources from each other, creating mini-perimeters within the internal network. A user or system does not automatically get to talk to a resource just because both are on the formerly "trusted" network. There should be a rule in place that defines who can access and under what circumstances. This leads to a lot of access rules and a lot of configurations to create, and that is not manageable in any type of manual or traditional manner. That is what has led to ideas such as Infrastructure as Code, which is what SDN is, just for network components. Technologies to support these ideas have followed suit.

Staying Afloat

Yes, there are newer challenges with greater interconnectivity. We want to embrace interconnectivity because we can be more productive, responsive and able to bring solutions to market faster. From that point alone, business is going to embrace greater interconnectivity. The key for us is to be proactive about understanding the technologies, the use cases and the ways we can put appropriate controls in place. Most solutions, even if cloud based, are fundamentally built on well-known architectures and patterns. When we understand those blueprints, we gain an understanding of where we are likely to find the issues with a given solution and what we can do to protect the organization. We learn the right questions to ask, the right evidence to examine and that means we can be faster at evaluating those solutions.

In addition, we can take advantage of the innovations in security and data protection that increased interconnectivity has birthed. A lot of these solutions fit with on-premises and hybrid modules of computing. Therefore, we can better protect traditional assets. We can apply the same types of rules and architectures across locations. And we can do it faster and far more efficiently than in the past. With a great deal of it defined by "code," we also can better examine and review given solutions, giving us additional confidence in our solutions. Overall, we can be more secure as a result. The more we take advantage of these security and infrastructure innovations, the fewer headaches those challenges cause us. That is how we stay afloat in this changing digital world.

Enjoying this article?

- Read *Risk IT Framework, 2nd Edition. www.isaca.org/risk-it-f2*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*