IT transformation through data security

Ensuring the continuous safety of your business

Table of contents

A primer on the IT transformation continuum: how security folds in

IT Transformation is a descriptor for the process of surviving and thriving in the Age of Digitalization, but the concept itself can seems like it's a one-time decision that immediately changes business technology operations from the ground up, which is rarely the case.

The IT Transformation Continuum addresses multiple infrastructures and workloads, intended to help identify where your business stands in the ongoing process of innovating, phasing out legacy systems and shifting operating models to excel in the digital economy.

For all businesses, regardless of industry, costs of traditional IT need to be minimized and reallocated into more innovative technology initiatives to help propel enterprises forward. People, processes and technology all come into play, and implementing efficiencies in each area is key to success. Teams must become highly efficient, technologies must empower people, and processes must be streamlined and automated to ensure superior functionality.

Wherever your business resides on the IT Transformation Continuum, making the necessary changes hinge upon three key areas of execution:

1. Virtualization

Technology comes into play significantly within the virtualization space. Leveraging virtual machines, containers and serverless technologies position your business to be more structured in all systems you build. Templates are used to spin up services, and from a security perspective, better enable you to be sure you have the right access lists, password requirements and more, built into your entire infrastructure from day one. Security becomes an integrated piece of your technology. Many security services available today are built cloud-ready and easy to consume.

- Containers
- Microservices
- Serverless computing

2. Integration

Integration is people-focused, particularly in the realm of DevOps, now often referred to as DevSecOps. Integration encourages your teams to think of security as an inherent part of everything they do. People are shifting their security activities from a siloed practice area that often gets attention reactively to thinking about the safety of workloads, applications, company and clients comprehensively.

- DevOps

3. Automation

Automation focuses on processes, and it's arguably the most important component of IT Transformation. Simply put, there's no technology on the planet that will protect you if you have a broken process. If it's within your power to automate a process, do so to ensure repeatability and reliability, security included. The ultimate goal is to reach an operating state that's expected, repeatable and enables the ability to be secure, reliable, and up all the time.

[1][Industry Report]: 2017 Thales Data Threat Report. Thales & 451 Research. Retrieved December 05, 2017 from https://dtr.thalesesecurity.com/.

[2][Industry Report]: What's Driving Boards of Directors to Make Cyber Security a Top Priority? Bay Dynamics. Retriever December 05, 2017 from https://baydynamics.com/resources/whats-driving-boards-of-directors-to-make-cyber-security-a-top-priority/.

Security landscape overview

Constant fear has spread throughout every industry due to the exponentially increasing amount of successful breaches and a threat landscape that swells daily with more malicious actors and new attack methods.

What does the security landscape look like? For starters...

88% of security executives feel vulnerable to data threats despite increased spending, Thales reported.[1]

Attackers stay hidden on a network for an average of 140 days before being detected, determined by Bay Dynamics.[2]

80-90 million cybersecurity events occur annually, with nearly 400 new threats every minute, WeLiveSecurity said.[3]

How are businesses being attacked? Most commonly:

- **Social engineering**
- **Unpatched software/OS**
- **Phishing attacks**
- **Denial of service**

In truth, most security downfalls are a result of inconsistent patching and failing to prepare engineers and users with proper knowledge through awareness and training.

What are some of the challenges we're all facing as a result? In summary, time, resources and money. Understanding environmental footprints and having clear comprehension on what's needed to get started are common burdens for many businesses. In-house experts are expensive and hard to come by, particularly when it comes to security.

- ISACA predicts there will be a worldwide shortage of two million cybersecurity professionals by 2019.[4]
- CyberSeek reported that each year, 40,000 jobs for information security analysts go unfilled.[5]
- Employers are struggling to fill 200,000 other cybersecurity-related roles.[5]

The skills gap alone is overwhelming. Meanwhile, security best practices are ever-evolving, threats change constantly and finding the best possible tools and expertise to support them within budget can seem like an uphill battle. Needless to say, the anxiety is understandable. However, we encourage you to take an accountable, pragmatic approach to security and embrace the evolution of your strategy with the components of the IT Transformation Continuum as your guiding initiatives.

Remember, hackers are always looking for your weakest link. Everyone wants to bring projects to the finish line, but don't do so at the cost of security. Stop and ask the fundamental questions: Is it secured? Has there been a security review? Have we encouraged user awareness and provided training? The most fundamental step you can take is making sure everyone is prepared on an ongoing basis.

[3]Thomas, K. (2015, September 11). The sad stats on state of cybersecurity: 70% attack go unchecked. Retrieved December 05, 2017, from https://www.welivesecurity.com/2015/09/09/cybercrime-growing-concern-americans/

[4][Infographic]: 2016 Cybersecurity Skills Gap. ISACA. Retrieved December 05, 2017 from https://image-store.slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dcbae-original.jpeg

FLEXENTIAL

Understanding the business challenges of security

Is your business a target?

It's a worthwhile question. Many decision makers agonize over their relative susceptibility to attacks, and the truth is, no one is immune from being targeted. That being said, upon examining the common themes of successful attacks and breaches, certain commonalities surface, and financial services, healthcare, and government are the verticals often mentioned.

The question then becomes, why are these industries and businesses being targeted? It's not necessarily the industries themselves; it's the data they're holding such as personally identifiable information, personal health information, research and development and intellectual property, in particular. These aren't the only things malicious actors are fixated on, but if you have multiple types of highly desirable data, then you're probably more susceptible.

According to the SANS 2017 Data Protection Survey[6], the following types of data were most commonly involved in reported breaches within the past 12 months:

42%
User login IDs and passwords

31%
Priviledged credentials

31%
Customer identifiable personal information

27%
Intellectual property

Regardless of industry, hackers have a wide range of motivations, and many attack at random. Some are simply seeking to create disruption within a certain industry or vertical. Others are focused on extortion and are primarily driven by money. The point is, while noting your respective industry and data types is worth doing, those things can't predict your precise likelihood of attack. You're better off focusing your energy on implementing a security policy and robust technologies that will help prevent, mitigate and remediate—the reality is, we're all targets.

Why security programs fail

While it's not possible to achieve a permanently secure state of operations, it's definitely possible to take maximum precautions. In many cases, attacks are successful because well-intentioned organizations fall victim to mistakes and oversight that are within their power to avoid. As mentioned, it often takes weeks and months of an attacker probing your network and perimeter devices to find vulnerabilities, and believe us, they're patient. The better you are at the basics of security, the easier it will be to detect intruders early on. While there are many potential security program pitfalls, here are three we see often:

1. **Poor patch management**
Healthy, consistent patch management is truly the low-hanging fruit of critical security practices, and it's also the low-hanging fruit of attackers. While staying on top of the number of patches necessary can be a lot to deal with, it will eliminate considerable risk.

2. **Failing at log management and event correlation**
Logs are incredibly important for the security team, whether from network devices, servers, applications or even printers. Analyzing logs can be focused on resource access, potential malware activity or authentication, and it assists security analysts with recognizing and responding to potential problems. SIEMS and event correlation go hand-in-hand with logging, allowing your security team to find out if certain suspicious activities are connected. Without these tools and practices, you're missing a lot of potentially critical information, and it will be significantly more difficult to find the source of security event.

3. **Not implementing monitoring and management**
Clearly, security tools are necessary, but they also have to be monitored and managed. Too often, an IT or security team will implement a particular tool, but fail to keep up with it over the long-term. Security tools have to be updated just like operating systems do.

When you scan the list above, what do all three errors have in common? Arguably, they could be boiled down to a lack of training and awareness. Within your organization, education must be constant. Security needs to be built into the culture of your business. The better your training, the higher the awareness of your employees. Technology is critical to security, but not without the support of your people and processes.

[5]Hack the Gap: Close the cybersecurity talent gap with interactive tools and data. (n.d.). Retrieved December 05, 2017, from http://cyberseek.org/index.html#about

[6][Industry Report]: 2017 SANS Data Protection Report. SANS and Infoblox. Retrieved December 05, 2017 from https://www.infoblox.com/wp-content/uploads/infoblox-whitepaper-sans-2017-data-protection-survey.pdf

Evolving your security strategy

Assess, plan, and implement

Every security program needs people, processes and technology to be successful. With these components to support you, you're on the right path to building an actionable security strategy. Remember that your plan is comprehensive and continuous, and it can be broken down into three cyclical phases:

Assess

Overall, assessment is focused on knowing what you have. Where decision makers often fail when taking on assessments is excessive focus on technology: appliances, applications and potential vulnerabilities. But it's the aforementioned people and processes that need the most attention. Don't get us wrong, technology is obviously critical, but it's useless without human beings and their methodology for operating it.

Another helpful part of assessing is ensuring that functional teams are aligned with security and meet regularly. Ideally, you should develop a security team and governance board designed to gain executive-level sponsorship.

Make sure that your IT and security team are also covering all areas of business. Shadow IT happens more often than it should, and if disparate departments are consuming IT services that IT isn't aware of, a vulnerability, breach or authentication issue could be how you find out. You should be reviewing controls, carrying out gap analysis and identifying your assets.

Plan

A great way to ensure adequate planning is putting together a steering committee to gain and maintain sponsorship of the executive team. Without their buy-in, ensuring your security program takes off will be like pulling teeth, if not impossible.

Processes are particularly important in this phase. Policy creation, incident response planning, and remediation and mitigation are all key. This phase is less focused on technology and more focused on how you'll ensure technology is supported.

Implement

The implementation phase is where technology plays the greatest role. Make sure you cover the security tools and tactics that are fundamental to safeguarding your business: multi-factor authentication, encryption, segmentation, role-based access, logging/SIEM, MDM and automation.

Education and training are also part of implementation. Provide plenty of security education and awareness training to ensure the success of your technology.

A few best practices

- **Don't store or handle sensitive data unless you have to**
- **Hire or build an internal security team**
- **Partner with a secure managed hosting provider**
- **Augment staff with professional services**
- **Employ hybrid strategies**

Flexential.com | sales@flexential.com | 877.448.9378