Secureworks®

CHECKLIST

Essential Actions for Protecting Business in the Digital Era: A Checklist

The potential benefits of digital transformation are supernumerous - it puts technology at the heart of an organization's products, services and operations, helping to accelerate the business and competitively differentiate itself through improved customer experience.

This is achieved using smarter products, data analytics and continuous improvement of products and services using software.

In order to digitally transform, organizations need to develop four competencies:

1. **Embrace software-centricity** across their products and processes
2. **Switch to greater use of sensors and instrumentation** across the business
3. **Be able to derive insights from all the data** available to the business[1]
4. **Leverage Cloud as a nerve cell of data analytics** for reporting back or taking rules and use cases.

These competencies should be foundational for planning your organization's digital transformation journey. As you embark on your digital transformation process, you must do it securely. To secure your digital transformation, you must understand with complete clarity and precision where you're going.

To put it simply, embracing digital transformation introduces a whole new set of technology problems. Therefore, you must first have the knowledge and expertise to solve those problems securely, or your digital transformation won't generate the value you intend.

Your business, IT and Security teams are embarking on a complex, ongoing journey. **Here are the essential actions you need to keep at the forefront of your digital transformation in order to effectively protect your business:**

☑ Understand where your digital transformation will lead you and the resulting security implications.

Clearly define goals for your organization. What are you hoping to achieve?

- Cost reduction?
- Higher efficacy?
- Increased efficiency?
- Improved functionality of applications?
- Access to better integrations?
- Deeper understanding of customers by leveraging IOT sensors?

The results of your efforts will suffer if you set a generalized goal of cost reduction, but don't clearly understand the available methods, or define the methods or expectations for evaluating exactly how the transformation is intended to cut costs.

✓ Define the security and functionality considerations of each technology you'll be introducing into your IT environment as part of your digital transformation.

Introducing new technologies into business is part and parcel to digital transformation. Your IT and Security team need to be fully educated on each digital transformation initiative and the technology that accompanies it. Security isn't about the perimeter anymore; it's a data-focused, people-focused objective of digital transformation itself. Be prepared to answer the following questions for any given piece of technology:

- Where is our data?
- What type of data is out there?
- How is data being handled?
- Who is handling the data on our behalf? (Cloud providers / third parties)
- What controls do they have in place?
- Are those controls sufficient to help us manage our cyber risk?
- Do the controls conform to both existing and newly-defined regulatory requirements that are changing with the initiative?

✓ Designate at least one SME and/or representative group for the ownership of each technology (including its subcomponents).

Moving to the cloud involves a paradigm shift in understanding that there are often a myriad of interactions and integrations underpinning each technology or service, breaking the traditional "silo" approach to technology operations. Even simple "lift and shift" moves to a single cloud provider involve a great deal of underlying technology. As such, one single person cannot own cloud as an initiative; it has too many complex parts, each integrating with one another and often differing substantially in approach or technology (or both) from that which is traditionally delivered or implemented on-premises.

With every move to a new digital transformation initiative, there's overarching technology, subcomponents, operational, and security aspects. Consequently, for every new digital transformation initiative to be implemented successfully, three to five people need to take ownership.

Very few businesses account for this in the pursuit of digital transformation and don't assign individual owners to focus on each part. We tend to think, "Well, we've switched substantial technologies before, we can do it again the same way." But, moving to the cloud involves more than just learning a new technology, it also involves learning new ways to think about how technology works, how it is applied, how it is secured, and what technology subcomponents make up the larger parts of every service. Each of these technological subcomponents require explicit focus, understanding, and ownership. The cloud as a whole cannot effectively support your digital transformation goals without explicit ownership to ensure each service and subcomponent is well understood, applied, integrated, secured, and continuously maintained and monitored for new or more effective capabilities.

✓ Ensure each of the following critical aspects of your security program are being properly and continuously prioritized, monitored and measured as you progress your Digital Transformation journey:

Data

- What type of data are you putting into digital transformation initiatives?
- Is that data sensitive in nature?
- Are you encrypting the data at rest?

Transmission

- How is the data being transmitted?
- Are you encrypting the data in transmission?

Applications

- What applications are you using in the cloud?
- Are these applications exposing your organization to more vulnerabilities?

Identity

- Who is accessing what information from where and why?
- How do you know they are who they say they are?

Authentication

- How are you granting granular controls for accessing various data types?
- Are you properly implementing Two-Factor Authentication (2FA)?

Endpoints

- How are virtual endpoints being monitored and secured?
- What external vulnerabilities are being brought in by external endpoints (IoT, BYOD)?

✓ Maintain appropriate security goals and metrics for each technology.

As you introduce new technologies, you will have additional points of monitoring and in turn more alerts. In preparation for and response to this, you will need additional subject matter expertise and staff who can add expertise to existing skillsets.

As you augment your security capabilities and staff, you'll want to consider the following key metrics (and questions to ask) to help assess the efficacy and efficiency of your operations:

- Ability to collect the data into a central view – visibility is key in your security transformation program
- True positive / false positive ratio
- Time to response (How long did it take from initial alert to first response action?)
- Efficacy of response (Did the response encounter unnecessary delay or involve incomplete actions?)
- Alert to personnel ratio (Do we have enough people to properly triage and investigate the vast number of alerts received?)

Back to the Why: Digital Transformation is for Creating Ongoing Benefits Specific to the Goals of Your Organization

You would think this would go without saying, but digital transformation shouldn't be done for its own sake. A lot of businesses are making massive technology moves, but why? What are the key indicators for decision making? What specific business, operational, and/or security objectives are you hoping for the cloud to help solve or assist with? When you're considering major technological transformation, the ultimate goal has to be bettering the business. Without goals or performance objectives, how will anyone know if it's a success?

The most successful early adopters of the cloud have clearly defined their goals, outcomes, and measurements well in advance, developing a clear view of intended benefits and the corresponding metrics by which they will be measured. They're able to collect the data and insights to show how a given digital transformation initiative has met, exceeded, or fallen short of the defined goals.

Furthermore, decision making is quickened as transformation progresses. A well-prepared business will meet growth targets at a lower cost and adapt to changing competition; the keyword here is "prepared." You must define success for your organization's digital transformation from the beginning.

Finally, the appetite for risk must inherently be increased. Time and money will be spent on work that may not benefit you in the long run; that's the truth. However, when initiatives with well-defined goals and measurements are intelligently executed, risk can be mitigated to an acceptable amount. The adoption of new technologies calls for a system of constant research, assessment, and verification. Business transformation is no longer about a single product as digital transformation isn't binary. Neither is it a single project that has an immediately defined start and an end. It's a way of doing business that comes with a change in culture. And, within any organization, the technology as well as the security requirements that underpin its long-term success will continue to evolve.

Want to learn more?
Click on the assets below to continue learning

Secureworks

ARTICLE

Defining Security Operation Methodologies for Better Expectation Setting from your Vendors

Secureworks

ARTICLE

Business Benefits Through "Smart Security"

Sources:

[1] Digital Transformation. (n.d.). Retrieved January 28, 2019, from https://www.dellemc.com/en-us/glossary/digital-transformation.htm

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp