FEATURE

4 top challenges to a secure digital transformation

Improving cybersecurity is becoming a driving factor for starting digital transformation projects. Mistakes in implementation, however, can be costly.

By Maria Korolov
Contributing Writer, CSO | SEP 12, 2018 3:00 AM PT

Digital transformation is vital to many companies' long-term survival, in that it can help them defend against agile startups, better meet customer expectations, find new opportunities, and reduce costs.

In addition, it can improve security. According to a survey 451 Research conducted late last year, 49 percent of IT professionals and line-of-business managers says that securing customer data is one of their main transformation objectives.

Research firm Lucid surveyed IT leaders this summer and, again, 49 percent of IT leaders say that better cybersecurity protection is one of the reasons their company is looking at digital transformation. (Lucid had not released the survey results at this writing.) Forty percent say that cybersecurity is the area of digital transformation their company is investing the most in.

"We are actually seeing more IT leaders take on digital transformation projects to support their cybersecurity strategies," says Monica Bush, director of security and compliance at Nintex, a security vendor that sponsored the survey. That includes everything from better access permissions during employee onboarding and offboarding, she says, all the way to big projects like tracking the location of sensitive data for GDPR and other compliance requirements.

In addition, moving to modern infrastructures, including cloud-based solutions like Office 365, can often improve security just by itself. Chad Weinman, VP of professional services at RiskLens, says that he's conducted risk analyses recently for large enterprises considering moving to cloud vendors. "We're going to be more worried about outages and data protection because our email environment isn't on-premises anymore," he says. "But what we've found is that the management of Office 365 by Microsoft is often far ahead of what the organization itself was doing, so overall, the actual exposure reduces when migrating to the cloud, rather than increasing."

Digital transformation projects could also lead to reduced visibility into the corporate environment, fewer human-powered checkpoints, and exposure to new kinds of threats, experts say. In fact, according to a recent survey by Fortinet, security is by far the biggest challenge to digital transformation efforts, with 85 percent of CSOs and CISOs saying it is a big hurdle.

Few companies are building cyber and privacy risk management into their digital transformation correctly, says Sean Joyce, US cybersecurity and privacy leader for PricewaterhouseCoopers in a recent report. "The winners of the future are going to be the ones that from the design phase all the way to production build in that risk management," he says. "it’s a brand-defining opportunity.”

Here are 4 significant challenges organizations face in building security into digital transformation.

Reduced visibility of data, processes

According to RiskLens' Weinman, when infrastructure is hosted by third parties enterprises typically have less control over what data they can collect. "If you host it on premises, you have really good visibility, can control conditions at any point in time, you have a lot of intelligence," he says. Vendors can provide some controls and reports, he adds, but not to the same degree as when a company controls its own infrastructure.

Visibility can also be a problem when a new system is installed locally as well, if the company doesn't plan ahead for managing the new infrastructure. "Every time you have an uncertainty as it relates to a state of an asset, or deploy new software to that asset, you open yourself up to risk," says Will Gragido, director of advanced threat protection at Digital Guardian. "Your attack surface increases."

Take containers, for example, which can be run in on-prem, hybrid, or cloud environments. "The failure to secure containers properly has been a problem for years," Gragido says.

One problem, he says, is that security isn't revenue-generating. "Most businesses don't make their money from security," he says. "So, historically, most people's primary concerns have not been in security, though it has improved over the years. As a result, infrastructures mature and get built out and grow faster, in many cases, than the companies can contend with from a security perspective."

The problem is exacerbated when the new technology is purchased by business units without input from IT. Cloud services in particular are fast and easy to set up and use without a lot of technical skill. "I have seen business units go off and build their own infrastructure," Gragido says. "They can't wait on IT. It's that old principle of not asking permission and begging for forgiveness later. That leads to problems." Companies don't have any visibility into systems when they don't even know that those systems exist.

Cutting humans out of the security process

Human employees are responsible for many, if not most, of the security problems in an enterprise. They make typos when entering transactions, they forget to enable security controls, they open phishing emails and click on malicious links, they fall for scams, and they insist on using the same insecure passwords everywhere.

"Oftentimes, our cybersolutions are more robust than we are, because we're easy to manipulate," says Trevor Brown, CTO at SecurityFirst. Human beings also provide a critical dose of common sense, he adds, and that goes away when processes are fully automated.

Take, for example, something as simple as a SQL injection. A human being can instantly tell a valid form submission from code without ever having seen the issue before, but a computer can only do it if it's been programmed to. "We look at something and get a gut feeling that something isn't right," he says. "Machines aren't good at that."

He's keenly aware of this problem, since his own company is in the process of increasing automation. "We're talking about this now with our own product," he says. "I can't have people at a console all the time in a high-efficiency, low-cost environment."

The unknown unknowns

Digital transformations can sometimes open new, unforeseen attack vectors. Take, for example, the use of Amazon S3 storage buckets. Cheap, convenient, easy to set up, easy to secure -- and easy to leave accidentally unlocked.

Over the past year, a large number of companies, including several very tech savvy ones, exposed sensitive data when they stored it on Amazon, including Accenture, Dow Jones, Verizon, and military intelligence agency INSCOM. Similarly, Kenna Security researchers recently found organizations leaking sensitive emails through public Google Groups settings. Organizations included Fortune 500 companies, hospitals, colleges and universities, and US government agencies.

"Google's G Suite is a product many transforming companies are moving to as part of their transformation," says Zia Hayat, CEO at Callsign, a London-based authentication technology vendor. "In fact, I was out on site with a customer just last week who uses

G Suite. But here again, misconfiguration in the form of a lack of ongoing vigilance has left a surprising number of organizations in diverse industries open to data loss."

You need a cybersecurity plan

CSOs have an important role to play in making sure that a company's digital transformation strategy includes a cybersecurity plan. They key to being effective, according to Hayat, is to focus on the issues that matter most to the company.

"I'm a security person," says Hayat. "And we like to talk in riddles. You need to put some clear and tangible examples out there that are not just technical but can show what impact something can have on your brand."

For example, he says, there's the impact of breaches on a company's market capitalization. "You can plot a simple graph of what was the cost to Equifax to its market cap, what was the cost to Target, what was the cost to Facebook in terms of its market cap from its negligence to consumer privacy and security. That cost has been increasing on a massive scale."

CSOs must also walk a careful line between being persuasive and being alarmist, says RiskLens' Weinman. Too many security professionals focus exclusively on the additional risks associated with moving data and processes to the cloud, for example, without considering the benefits.

"This isn't actual analysis work, it's spreading fear, uncertainly, and doubt and can lose the CSO credibility with the business," Weinman says. "Then business is still likely to be doing the project because they see value, opportunities, or cost savings -- and the CSO gets sidelined."

If the CSO can objectively talk about risk and security in business terms, they're more likely to have an impact, Weinman adds. He suggests that security professionals look to international standards in risk assessment, such as the FAIR risk assessment framework. "It's not about the FUD, or that the cloud is dangerous," he says. "But about helping make a well-informed decision."