Digital transformation and risk management must go together

Light Dark

October 6, 2022

By George Platsis

4 min read

Risk Management

The recent PwC 2022 Global Risk Survey gives a glimpse into what senior leaders think about their business efforts. The report opens with some expected highlights worth repeating:

- Change is increasingly fast and disruptive
- The COVID-19 pandemic caused disturbances in the labor and supply markets
- Geopolitical risk is on the rise
- New regulations, including an increased emphasis on risk, audit and compliance issues, refocus and redirect organizations' priorities
- Supply chains, cyber risks and public safety issues all feel pressure from the above factors.

In view of these issues, digital transformation and risk management are more important than ever. What's the difference between them, if any? In fact, they are much more closely linked than their names suggest.

Can you blindly transform?

In a word: yes. Whether that is a sound business decision is a different issue. As we noted before, there are many different puzzle pieces to strengthening an organization, but those different pieces have connective tissue: the risk assessment.

You see, a strong risk management program gives an organization a sober and clear-sighted approach to its decision:

- When to spin off a business unit? What are the risks to brand, reputation and cash flow?
- How about a multi-year digital transformation project? What qualities are we looking for in vendors? How will operations be impacted? Are we future-proofing ourselves with a solution that can ore than a few years?

These simple examples illustrate that at the heart of any strategic issue, there is some underlying risk issue, too. And, as we previously saw, program maturity and posture will be driven in large part by the organization's risk appetite. Running a digital transformation strategy is no different.

Complex problems, simple solutions and difficult implementations

You have probably seen a 'heat score' matrix in your professional travels. They're color-coded scores, translating some qualitative assessment into a quantitative score, used to make quick decisions. In the heat of the moment – for example, during an incident response or crisis management scenario – these matrices are excellent tools. They don't work as well for strategic planning, though.

Complex problems do not always require complex solutions. In fact, simple solutions are likely best, with the caveat that difficulty and complexity could come with implementation. For example, I know I need to go from point A to point B (the simple solution that gets me out of my complex problem), but going on that journey may be very difficult.

Remember, decision-makers do not have the time, and perhaps neither the patience nor tolerance, to navigate a complex or over-engineered solution. A board or C-Suite may need core questions answered, such as:

- Are the right defenses in place and the right resources at hand?
- Do the people who require permissions have them?
- Will the solution impede our business needs?
- How does this solution grow our business?

They want to know the details of the journey (point A to B) and not every [illegible] he way, even if prudent planning requires it. In the end,

risk management are connected, so we need a basic framework to tackle the complex problem.

Bringing it all together for cyber resilience

So, what can we use for strategic planning? We already have a good primer. Here is a recap:

1. Know your resources
2. Define your risk posture
3. Get in the right frame of mind
4. Step up to the challenge.

As basic as these steps may appear on the surface, they are deep and loaded with intricacies. For example, you will have technical challenges, such as defining your disaster recovery capabilities pre- and post-change. Or, you may need to assess the chance of deploying 5G/edge solutions or whether artificial intelligence is right for you.

Then, there are non-technical challenges that will require your chief information security officer to bring out their best game. Technical and non-technical staff will be forced to speak a common language, almost always dollars and cents.

Apples to apples

And there is one of the keys to success: commonality. In order to make sound decisions, you need to trust people are talking apples to apples.

There are some great industry frameworks out there – such as NIST SP 800-30, SP 800-34 and ISO 22301 – which focus on risk management and business continuity. Whichever framework you have deployed, there are a few things that need to happen in order to be successful:

something is a risk, but another does not, you have a problem. Definitions matter and precision in language matters. Having a single pane of glass for common reference is crucial.

- **Governance.** Is there any formal program in place, even if not running at its best? A formal program tries to distribute ownership and enforcement. It also shows some leadership buy-in already exists.
- **Collaboration.** If specific teams don't talk to each other, any effort is doomed to failure. For example, the technology and infrastructure team may want to make a wholesale move to the cloud. However, the business team may find that a business risk the organization cannot take on (say, for example, if a key selling point of the service is that nothing is cloud-based). These are the types of nuances that turn well-meaning efforts into potential business disasters.

Useful data to make informed decisions

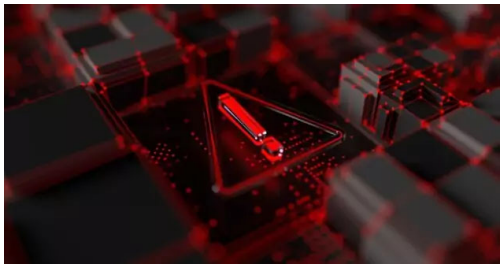
Common understandings are the key. The benefits can be extremely positive if they exist and consequences downright painful if they do not. Your staff and decision makers can get stuck on trying to make sense of what 'risk' means. Definition and precision will prevent that.

In closing, digital transformation can happen without risk management, but it is risky. Conversely, if your risk management program isn't informed by transformation strategies, it could be a possible opening waiting to be exploited. In the end, you can't do one without the other.

digital transformation | Risk Assessment | Risk Management | Security Risk

CONTINUE READING

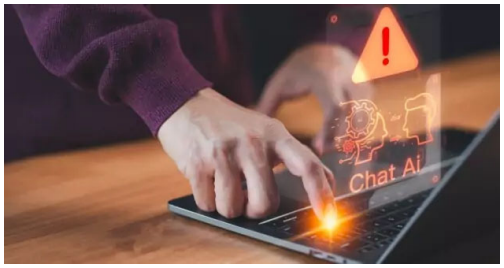
POPULAR



ARTIFICIAL INTELLIGENCE | April 30, 2024

AI cybersecurity solutions detect ransomware in under 60 seconds

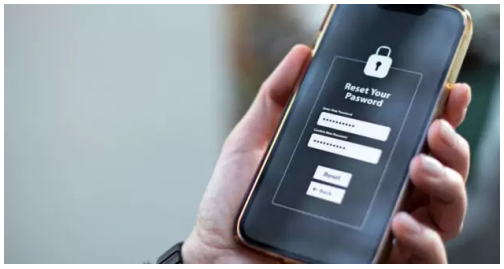
2 min read - Worried about ransomware? If so, it's not surprising. According to the World Economic Forum, for large cyber losses (€1 million+), the number of cases in which data is exfiltrated is increasing, doubling from 40% ...



RISK MANAGEMENT | April 24, 2024

Researchers develop malicious AI 'worm' targeting generative AI systems

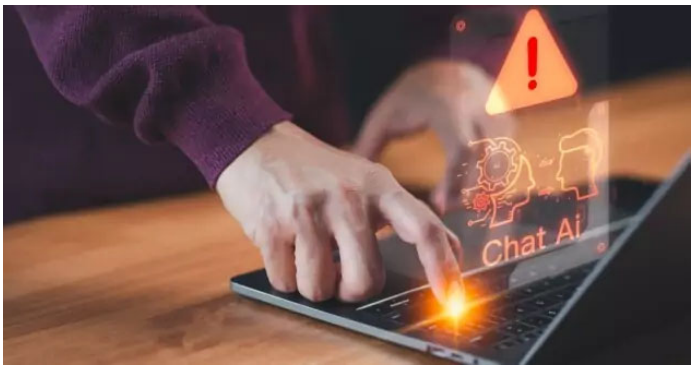
2 min read - Researchers have created a new, never-seen-before kind of malware they call the "Morris II" worm, which uses popular AI services to spread itself, infect new systems and steal data. The name references the original...



IDENTITY & ACCESS | April 23, 2024

Passwords, passkeys and familiarity bias

5 min read - As passkey (passwordless authentication) adoption proceeds, misconceptions abound. There appears to be a widespread impression that passkeys may be more convenient and less secure than passwords. The reality is...



April 24, 2024

Researchers develop malicious AI ‘worm’ targeting generative AI systems

2 min read - Researchers have created a new, never-seen-before kind of malware they call the "Morris II" worm, which uses popular AI services to spread itself, infect new systems and steal...

April 17, 2024

What should Security Operations teams take away from the IBM X-Force 2024 Threat Intelligence Index?

3 min read - The IBM X-Force 2024 Threat Intelligence Index has been released. The headlines are in and among them are the fact that a global identity crisis is emerging. X-Force note...

April 16, 2024

Obtaining security clearance: Hurdles and requirements

3 min read - As security moves closer to the top of the operational priority list for private and public organizations, needing to obtain a security clearance for jobs is more commonplace. Securi...

Topic updates

Get email updates and stay ahead of the latest threats to the security landscape, thought leadership and research.

Subscribe today →

Analysis and insights from hundreds of the brightest minds in the cybersecurity industry to help you prove compliance, grow business and stop threats.