Embedding cybersecurity into digital transformation – a journey towards business resilience

All organizations face a wide range of risks that can cause financial loss and reputational damage, from natural disasters and market turbulence to cyber threats and associated technology disruptions. With organizations facing constant changes in the market, business resilience is no longer just about the ability to adapt and recover from disruption, (business continuity planning) but being able to anticipate and prevent any disruption in the first instance.

A resilient business will combine business continuity planning with risk management planning to better navigate disruptive change and protect shareholder value. As the world becomes more turbulent, organizations need to accelerate their business resilience planning.

As organizations continue to expand their digital footprint, the risks associated with digital business are increasing in quantity and complexity and the need to provide continuously available services to customers requires organizations to become more reliable and more resilient. It's increasingly important, therefore, to embed security solutions and processes into the very fabric of the business and to secure these digital assets in order to mitigate the risks. Today's organizations will never be adequately business resilient, if they ignore or underestimate the need for robust cybersecurity planning.

Embedding cybersecurity into digital transformation projects

When an organization promises to deliver the value of digital business to customers, it's often the case that security professionals are not at the table when critical decisions are being made. And without security professionals in the room at the right time, organizations are exposing themselves to business critical risks that could damage the brand.

We're already at the point where organizations are relying on their digital capabilities and any downtime is untenable, not to mention costly. Yet digital projects continue to grow in number and many of these are happening outside the IT department. Gartner predicts that in 2017, 50 percent of IT spending will be outside traditional IT departmental control.[1] This growing trend is creating new challenges for the business and if cybersecurity measures are not embedded early, the organization will face issues relating to security, risk and privacy.

Digital transformation covers a number of key project areas including:

- Hybrid cloud and virtualization projects, taking advantage of the cloud and virtualization to drive cost savings, flexibility, and business continuity planning
- Customer experience and analytics, with projects aiming to harness the power of business intelligence utilizing big data analytics
- Digital infrastructure projects which use a combination of data and analytics to unlock key business information and drive growth
- Creating tomorrow's workplaces – blending mobility, communications, and collaboration.

Such projects are complex, costly, and have interdependencies and inherent risks associated with them. Managed and executed well, they will contribute to building a resilient business – one that can protect its assets from cyber threats and respond quickly to attacks. And to manage them well means embedding cybersecurity from the outset, resulting in a more integrated way to manage broader business resilience.

> **To really claim to be business resilient, every project needs to start with the same question. Is the system secure?**
>
> Garry Sidaway, NTT Security

Putting a value on business resilience

Calculating the cost of downtime isn't simple – you know that it costs you, but how do you really estimate the lost revenue, reduced employee productivity, lost commercial opportunities and damage to your brand? Persistent ransomware attacks on businesses around the world have shown the disruption that can be caused to business operations, lost business opportunity due to downtime,

1. Gartner press release 'Gartner Says Digital Business Economy is Resulting in Every Business Unit Becoming a Technology Startup'

and the financial impact of paying large sums of money to cyber criminals who have held their data to ransom.

Data breaches alone are estimated to cost an organization in the region of $1.3 million according to NTT Security's Risk: Value Report 2017, and 57 percent of respondents in the same survey believe a data breach is inevitable. Surprising then that many organizations are still setting unrealistic timescales for digital transformation projects rather than building in sufficient time to build in cybersecurity capabilities.

Resilience isn't only about catastrophic threats, it's also about everyday and continuous threats.
Peter Firstbrook, Gartner[2]

Make security the starting point, not an afterthought

Despite all the talk of cybersecurity capabilities being built in versus bolted on, security remains an afterthought for a vast majority of digital transformation activities such as mobility, cloud services and customer experience programs. Too often, security is seen as slowing down a project rather than enabling its success, and with time pressure to get a project up and running, the lack of sound security considerations is a problem for organizations striving for true business resilience. With the increasing regularity and publicity of cyber attacks, businesses must realize that their customers are more aware of cyber issues than ever before, making embedded security a critical competitive advantage.

The results of a recent survey[3] highlighted that only 18 percent of organizations agreed that their security team had been involved in all their digital transformation projects, and 76 percent agreed that security considerations were added too late in the project, meaning that projects needed to be retro-fitted after key decisions had been made. In the same survey, 85 percent of respondents agreed that the security team could have done a better job if they had been included earlier in the project. The key challenge for the security team is to reassure the business that Secure IT and IT are the same thing and no digital transformation project should ever start without understanding its security implications.

Consideration should be given too, to the strategy for purchasing IT solutions and security solutions. Multiple suppliers can result in a complex process for integrating systems, therefore having an orchestrated IT governance model with embedded specialized security can help to transform your digital business and at the same time, secure it.

The benefits of integrated cybersecurity

Integrating cybersecurity processes from the outset can strengthen digital transformation projects but organizations are at different stages and need to work with the right experts to navigate the options available to them no matter which stage they are at on their journey. Choosing the right team of experts to tightly integrate cybersecurity into your digital transformation projects will enable you to:

- Address risk management through an integrated approach using a combination of consulting services, managed security services and technical security – to enable you to identify and control risks
- Reduce the complexity of your security architecture and operational model
- Add value to the digital business planning team to help them build resilience into the project, by assessing business risk and procedural controls
- Prioritize areas of business critical risk
- Write a cyber resilience plan using language that the business will understand
- Create greater customer satisfaction, loyalty and trust among your stakeholders
- Tightly embed seamless security, without delay to project timescales and allowing businesses to be quick to market
- Develop an integrated approach to cybersecurity to reduce your organization's risk footprint. This will enable you to detect increasing cyber threats and if necessary, recover quickly and efficiently from a breach
- Understand the cyber defence maturity of your own business and implement an architecture that will help you prioritize investments, align them with business objectives and keep ahead of regulatory and compliances pressures.
- Implement applied threat intelligence into your security to ensure IT is resilient against the latest threats
- Seamlessly protect your environment from adversaries looking to exploit vulnerabilities as you transform your digital assets.

Conclusion

Ensuring that cyber risk management is part of your business resilience plan is not something that can be added after the event. It must be included from the outset and embedded across the organization, from your technologies right through to your culture. Today, the pressure in the digital economy is to be 'always on', offering a continuously available service to customers. And that means that – more than protecting the enterprise – the challenge now is to ensure its resilience.

By 2020, 60% of digital businesses will suffer major service failures due to the inability of security teams to manage digital risk.
Gartner[4]

About NTT Security

NTT Security is the specialized security company of NTT Group. With embedded security we enable Group companies (Dimension Data, NTT Communications and NTT DATA) to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of consulting and managed services for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more.

To learn more about NTT Security and our unique services for information security and risk management, please speak to your account representative or visit: **www.nttsecurity.com** for regional contact information.

2. The Six Principles of Resilience to Manage Digital Security 3. Digital Transformation Security Survey 2016: Dimensional Research, sponsored by One Identity
4. Press release: Gartner Special Report Cybersecurity at the Speed of Digital Business