Capgemini invent

Digital Trust & Security - Securing Digital Transformation

CONTENTS

EXECUTIVE SUMMARY

Digital Transformation provides companies with many new opportunities to design their products and services in ways that shape competitive advantages. At the same time, it brings considerable Digital Trust & Security risks, as new technologies open up organizations to all kinds of attacks. The types of threats and risks depend on the technologies at hand, yet it is clear that no technology can be perfectly secured.

Digital Trust & Security must become an essential part of every company's Digital Transformation strategy, as ignoring associated risks may have significant reputational, legal, and financial consequences. As complete protection is impossible, organizations should focus on minimizing the impact of breaches. This approach requires a change of perspective on Digital Trust & Security: a paradigm shift. This shift takes place along five lines:

1. Companies should let go of the zero-risk dream and focus on recognizing digital risks and the variation of importance of data assets over time – the information life cycle.
2. They should focus on data-centric defense instead of perimetric defense, aligning efforts to identify and protect the data assets that are most valuable to the company at that time.
3. They should look at Digital Trust & Security as less control-centric but more people-centric and take a security by design perspective: Digital Trust & Security becomes an enabler and valuable development partner rather than a gatekeeper.
4. Instead of thinking about Digital Trust & Security in the traditional way of preventing and protecting, companies should aim to predict, monitor, and respond to threats and attacks.
5. To free up time of security specialists to add value to the company, manual execution of tasks should be limited, with as much automation and intelligent execution as possible.

These measures help companies change their mindset with respect to Digital Trust & Security. The following approach helps them to put secure Digital Transformation into practice:

1. Conduct a digital and Digital Trust & Security maturity assessment
2. Identify and balance risks & opportunities
3. Define and align digital and Digital Trust & Security strategy
4. Derive the roadmap for a secure Digital Transformation
5. Establish a security mindset and sustain the change

1. DIGITAL TRUST & SECURITY AND THE PRESSURE TO INNOVATE

Technological developments are transforming the way we interact and communicate with each other and with the world around us. Amazon, for example, has completely changed how people approach shopping, while Uber and Lyft have reinvented ride sharing. Disruptive innovations like these affect all three digitally and economically relevant dimensions of a company: business models, operational processes, and customer experience. Companies see themselves forced to radically rethink their business as ambitious competitors chip away at their market share by delivering improved and new products faster and better through smart innovations. Those who do not move quickly and leverage technological developments risk vanishing into economic insignificance. Therefore, the question of realizing Digital Transformation is not a question of choice - it is an imperative.

Cyber Threats are Growing

Technological developments have not only radically increased the number of business opportunities for companies to find, the number of Digital Trust & Security threats has grown exponentially as well. Worldwide, the average number of targeted cyber-attacks per company almost doubled between 2017 and 2018. Threats come in many guises, including employees, potential clients, hacktivists seeking recognition, suppliers, criminal organizations, and even state-sponsored attacks. Recent years have shown some of the largest data breaches in history. The infamous WannaCry and Petya ransomware attacks locked hundreds of thousands of users out of their computers. The Equifax breach laid bare sensitive personal data of nearly half the US population. Other recent victims include Marriott International (500 million records compromised), Yahoo (3 billion+), Facebook (50 million), and Cathay Pacific Airways (9.4 million).

Consequences of these attacks can be severe: loss of consumer trust, theft of intellectual property, and service disruption only scratch the surface of the risks that firms are exposed to. Important data protection regulations to protect consumer privacy have been put in place in recent years that require companies to pay close attention to how they handle data. Non-compliance poses another grave legal, operational, strategic and reputational risk.

Today, the threats are more pertinent than ever as organizations of all sizes seek to transform themselves to take advantage of new technological developments. They adopt so-called SMACT-technologies and implement organizational changes. As a result, the number of interfaces – attack points – rises, which can increase the possibility of exploitable vulnerabilities in the IT-infrastructure or organization. In their focus on finding the Next Big Thing, companies often fail to take note of these cyber threats. Balancing the benefits of Digital Transformation with security requirements is one of the most difficult tasks of a business leader. Yet, in firms of all sizes and in all industries, Digital Trust & Security cedes priority to Digital Transformation. The question now is: what can an organization do to balance Digital Transformation and Digital Trust & Security? To answer this question, an understanding of the implications of Digital Transformation is essential.

WannaCry was a global ransomware attack in 2017 that exploited a vulnerability in older Windows operating systems. Infected computers were encrypted until a ransom in Bitcoin was paid to the attackers. The attack affected more than 200.000 computers in 150 countries. Many of the affected organizations, including telecommunications companies, hospitals, and banks, were forced to completely replace their IT systems. Cost estimates vary into the billions of US dollars. Unpatched systems are still vulnerable to the ransomware.

2. DIGITAL TRANSFORMATION: DEVELOPMENTS AND IMPLICATIONS

TECHNOLOGICAL TRENDS AND IMPLICATIONS

In the past decades, digital developments have radically transformed the world. New technologies and resulting organizational structures have come to form an integral part of modern life. While the Digital Transformation has led to an incredible number of business opportunities, it has completely changed risks people and companies are exposed to. This is not a static change, as technological and organizational trends continuously change the way people work and share information. Digital Trust & Security development must keep up with these trends to stay ahead of implied threats.

Social Media

Both in private settings as well as in the work sphere, social media provide convenient means of communication and collaboration. However, these communication platforms come with a risk. People share unprecedented amounts of personal information through these services, blindly trusting the platform to safeguard their information. At the same time, people expect the same convenience in their work as they get from the communication platforms they use in their private lives, such as WhatsApp and WeTransfer, that enable them to share information and documents with ease. If this need is not met, people often defer to their preferred applications. As a result, company information can slip from the company's radar, at risk of leaks, reputational damage, and heavy fines under data protection regulations.

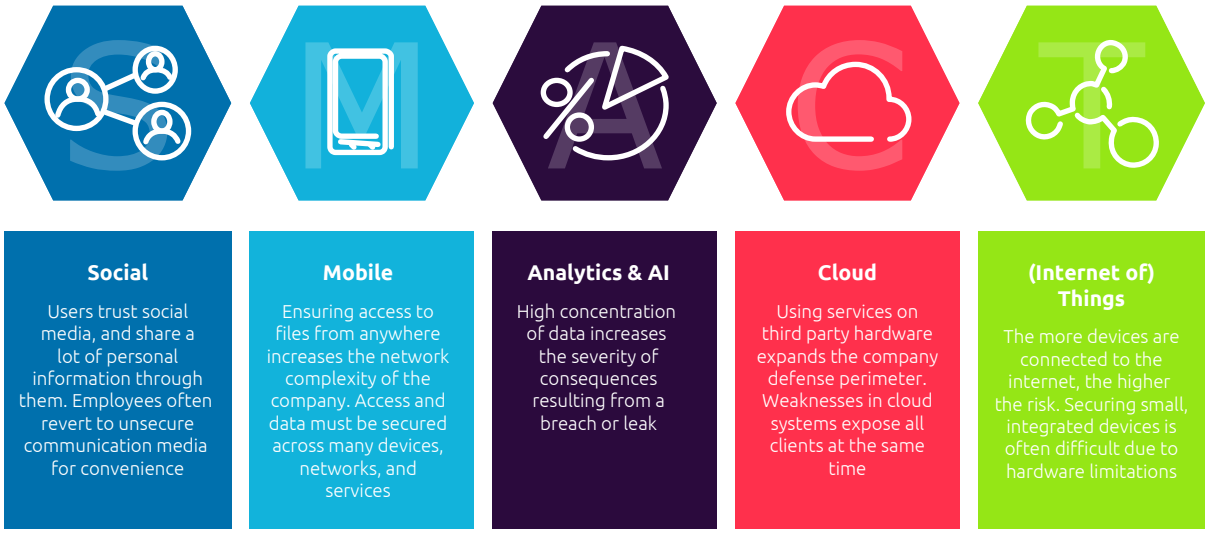
Mobile

Employees expect to have access to company services anywhere they go, always. They want to use their device of choice to access these services. The challenge is to secure communication between an enormous number of different devices, using all kinds of platforms on many different networks, while ensuring usability. Both the communication sent from mobile devices as well as the device itself pose risks, as laptops, tablets, and phones can be lost or stolen.

Analytics & AI

Analytics & AI technologies are used to analyze consumer behavior, improve chatbots and conversational UIs such as Alexa, or to find new business opportunities. The level of personalization and customization that consumers demand from services keeps increasing. Never before have companies collected, processed and stored as much data as they do today to meet these needs and improve

Figure 1: Technological Trends and Implications



their market position. Companies often start collecting as much data assets as possible before they identify opportunities on what they can and want to do with them. The greater the amount of sensitive data collected and stored, the more severe the consequences of a breach can be.

Cloud

To meet market needs and stay ahead of the competition, with margins shrinking and fickle customer loyalty, companies look to break the value/cost trade-off. Cloud applications or Anything as a Service (XaaS) solutions are attractive options in this transformation, as they offer flexibility and cost reduction at the same time. Substantial expenses on equipment, maintenance, and upkeep can be avoided by using third-party hardware solutions. Many of these services move the processing and storing of data to third parties outside of the company perimeter. At the same time, a breach of the cloud service provider puts all their clients at risk, since they use the same hardware and infrastructure. The security of these third-party services thus becomes essential to the company's own Digital Trust & Security. Due to the complexity involved in sharing hardware among many different clients, a high level of Digital Trust & Security knowledge is required to manage a potential breach.

Internet of Things

The number of everyday objects that are connected to the internet is increasing exponentially. These connections offer a great many opportunities from package tracking to vehicle maintenance prediction. The number of applications is only matched by the amount of Digital Trust & Security risks that arise with them. IoT devices often connect by hardware of limited capabilities that do not always allow for advanced encryption and security mechanisms. Hackers can take advantage of these weaknesses and potentially take control of, for example, a connected car, with devastating consequences.

ORGANIZATIONAL TRENDS AND IMPLICATIONS

Organizational Structure

The Digital Transformation has led many organizations to change their organizational structure to stay ahead of the competition, placing the customer at the center of all actions. To faster react to customer demands and changing market requirements, companies move towards increasing the number of teams within the organization while reducing their size. Each team has more specific responsibilities and a higher level of decision-making authority. In many cases, each team is responsible for establishing its own technical architectures focusing on a delivery on microservice level. This level of autonomy leads to challenges for Digital Trust & Security compliance, awareness, and consistency between the teams, as their understanding of Digital Trust & Security requirements, their working styles, and the systems used may vary greatly from team to team depending on which SMACT technologies they use.

Workforce and Skills

As technological developments accelerate, technologies used in people's work and private lives change more rapidly and become more complex. People's understanding of new technologies often lags behind the speed at which the technologies develop. In some companies this problem is larger than in others, especially when they have an aging workforce. As people live longer lives and retire later, this means that an increasing number of workers will be forced to work with technology they cannot or do not want to fully understand. At this point, the risk emerges that people will continue to use outdated systems, or they use new systems without realizing the associated Digital Trust & Security implications. Over time, the skills present within the company to leverage technology for the firm's benefit diminish in value and need to be addressed.

Employee Expectation & Power

Recent years have seen increasing competition for talents. Talent acquisition and retention have become central to a company's success. Driven by employee needs and wishes, firms must adapt how they organize the working environment they offer. From an IT perspective, employees expect to take the convenience of the services they use at home to the work floor. If this demand is not fulfilled, they will bring these services with them. At the same time, employees usually get extensive access rights to impressive amounts of data to facilitate work efficiency. In the work sphere, then, private and company data meet and mix. This poses risks if employees

are not trained sufficiently to handle company data properly. Humans have been the main vulnerability in most recent Digital Trust & Security breaches. Employee awareness plays a crucial part in preventing them.

Agility

Firms that aim to come out on top through Digital Transformation use agile working styles to meet the increased dynamics of the market. Small agile teams are given responsibility and decision rights. At the same time, they are under pressure to perform well and quickly. Delivering new product features often takes priority over security implications. As a result, risks are being accepted to come up with innovations faster. While there are some security rules within agile development, because of the time pressure involved, agile is often misinterpreted to mean undocumented or rules-free. This area of conflict must be resolved to support the secure Digital Transformation.

Digital Product Development

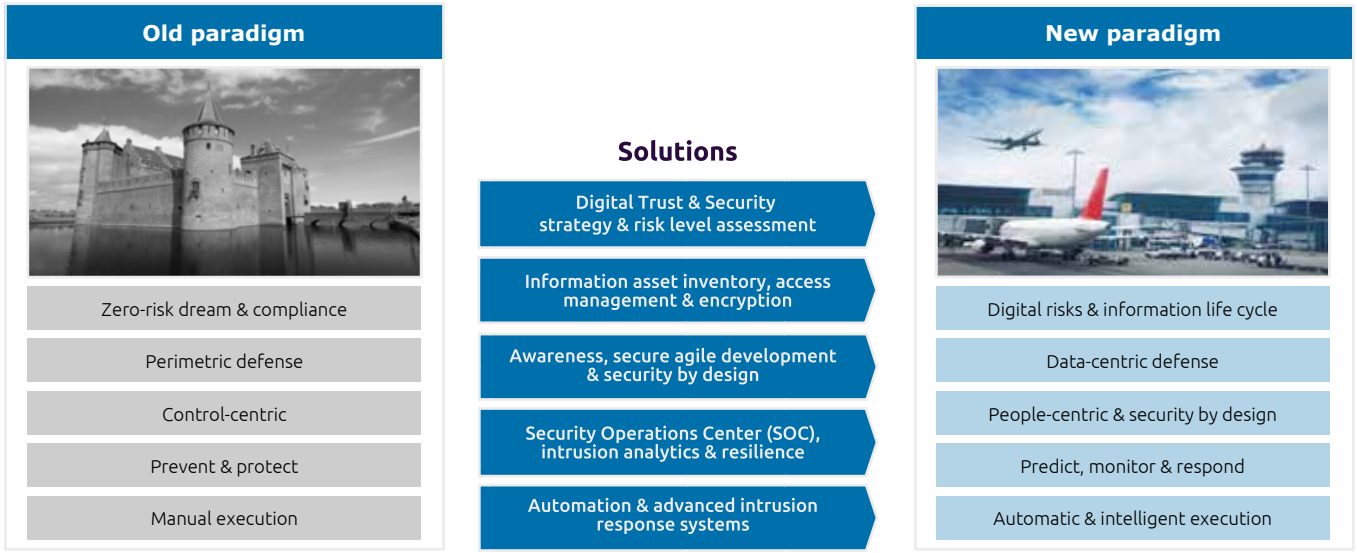
In software and digital development, combined development and operations (DevOps) teams are formed to drastically reduce delivery and maintenance times of software products. The speed at which DevOps teams work is often too high for traditional security departments to keep up, which forces traditional Digital Trust & Security compliance to the final gate of the development process, with significant time costs for both the security and DevOps teams. Organizations must adapt their Digital Trust & Security functions to this change. Additionally, products can be developed from anywhere by using collaboration tools and methods. Besides the vulnerabilities of these tools, developing at remote sites or in public poses further risks: lost or stolen devices and documents as well as eavesdropping and spying can compromise sensitive information.

Figure 2: Organizational Trends and Implications

3. A PARADIGM SHIFT IN THE WORLD OF DIGITAL TRUST & SECURITY

The Digital Transformation has brought important changes to how firms look at business models, operational processes, and customer experience. They must redesign their thinking about Digital Trust & Security to meet the challenges posed by these changes. Old ways of defending company systems no longer suffice to protect critical assets. If the old world resembles a castle that can be protected by a moat and a wall, the new world is like an airport, where walls have little to offer. This paradigm shift takes place along five different dimensions and requires organizational as well as technical measures to succeed.

Figure 3: From the Zero-Risk Dream & Compliance to Digital Risks & Information Life Cycle



FROM THE ZERO-RISK DREAM & COMPLIANCE TO DIGITAL RISKS & INFORMATION LIFE CYCLE

The zero-risk dream is over. Organizations must make moves to accept digital risks and focus efforts on dealing with them, as preventing them completely is simply not possible. Therefore, it is crucial to smartly define which data requires protection most, the so-called crown jewels, and focus resources on safeguarding its flow across devices, the cloud, and internal systems. To this end, companies should conduct a risk-assessment and prioritize measures to mitigate the greatest risks associated with each new service that is developed or integrated. Throughout this process, it is important to keep in mind the life cycle of each piece of data to assess what information is most important at any point in time. So, how should organizations go about adopting a digital risk and information life cycle perspective?

Integrate Digital Trust & Security into the Company Strategy

ORGANIZATIONAL

A central Digital Trust & Security position should be part of the company board, equipped with adequate means for governance, process, and technological security measure implementation. Additionally, Digital Trust & Security representatives should be part of every business area to help these departments to keep its importance in mind. They actively participate in reaching the department and adapt security guidelines to local needs.

Assess Risk Levels Continuously along the Information Life Cycle

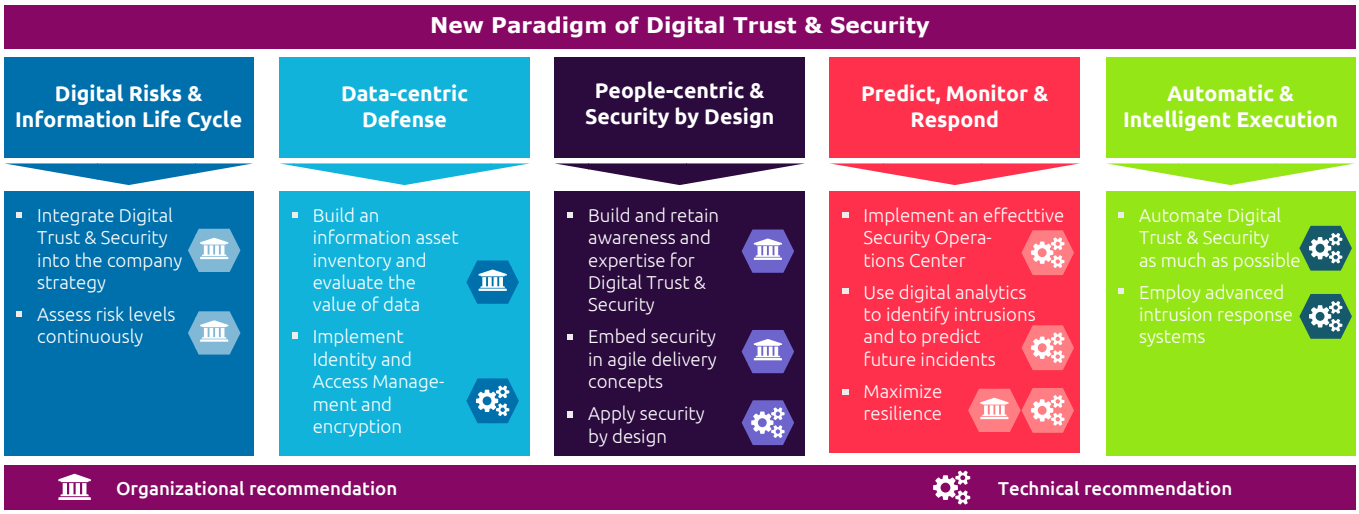
ORGANIZATIONAL

Organizations must analyze the Digital Trust & Security risks that they are exposed to through all of their systems. In this analysis, it is important to be aware of the life cycle stage that each information asset is in, as the value and sensitivity of these assets change over time. A comprehensive Digital Trust & Security risk assessment enables the enterprise to:

- Identify Digital Trust & Security risks regarding the company's systems, assets, data, and capabilities
- Implement steps to protect the enterprise and ensure continued operations
- Develop capabilities to detect a Digital Trust & Security incident
- Implement appropriate steps to respond to incidents and security events.

IT and the business should jointly identify and evaluate cyber risks as part of a company-wide standardized risk management process. The same procedures and tools should be applied across all departments, so their risk assessments can be compared. As resources are limited, not all risks can be addressed. The risk assessment helps decide how to allocate them to protect the most critical assets best.

Figure 4: New Paradigm of Digital Trust & Security



FROM PERIMETRIC TO DATA-CENTRIC DEFENSE

Traditionally, a firewall was enough to keep most intruders out. Modern business requires constant connections between interfaces, platforms, and devices. As a result, the borders between internal and external networks have become blurred, and the security perimeter no longer ends at the door, but extends to all third-party services and devices the company is connected to. Achieving one hundred percent protection has always been impossible. With this increased perimeter, however, it has become even more challenging. So, how can a company achieve a data-centric defense perspective?

Build an Information Asset Inventory and Evaluate the Value of Data

An information asset inventory provides organizations with a comprehensive overview of their digital assets and the values and risks associated with them, as well as an overview of responsibilities and data owners. Appropriate security levels are assigned to each piece of data based on their confidentiality, integrity, and availability from a business perspective. Then, the so-called crown jewels are identified: essential digital assets that are crucial to the firm's operation. As a positive side-effect, future data strategy and governance will benefit from this overview.

Implement Identity and Access Management, Encryption, and Data Leakage Prevention Measures

Identity and Access Management (IAM) ensures that adequate user access roles and rights are defined and continuously updated when employees change roles or leave the company. Furthermore, sophisticated encryption helps alleviate the severity of unavoidable breaches. Finally, adequate data leakage prevention measures, such as document monitoring, help avoid sensitive data exposure.

FROM CONTROL-CENTRIC TO PEOPLE-CENTRIC & SECURITY BY DESIGN

Humans are the source of Digital Trust & Security vulnerabilities in the majority of known cases. Organizations should acknowledge the importance of the human factor in the fight against cyber threats. The spoilsport, gatekeeping approach that Digital Trust & Security departments are traditionally known for does not work. Instead of forcing compliance with controls and regulations, Digital Trust & Security representatives should focus on enabling product development and establishing awareness among colleagues. The following recommendations will help organizations to adopt a people-centric and enabling perspective.

Build and Retain Awareness and Expertise for Digital Trust & Security

Sustainable establishment of Digital Trust & Security measures depends on the support of employees for the implementation, execution, and maintenance. The people-centric approach requires all employees to be trained in Digital Trust & Security. They should all understand potential cyber threats and their role in preventing them. Creating this level of awareness goes beyond one-off training sessions: as cyber threats and security measures continuously change, employees should be trained accordingly.

Embed Security in Agile Delivery Concepts

Companies striving for digital leadership turn agile to accelerate development. Development teams are given significant decision power to enable their progress. The pace at which teams form and dissolve, as well as the impressive number of different projects running simultaneously provides a challenge to Digital Trust & Security, since that is rarely a high priority within agile concepts. In this context, agile means fast throughout times for decisions. Digital Trust & Security must advance accordingly: it should be integrated from the start of the project, with security sprints as part of the development process, and the outlining of minimum security requirements. Awareness among developers is essential, and Digital Trust & Security experts must be trained to add value to agile teams.

Apply Security by Design

Security by design is about thinking ahead and about building security into each part of the organization and its digital products right from the beginning. The goal is not to completely prevent malicious attacks, but to minimize the consequences of such an attack to the business. Incorporating security right from the start enables more secure growth and significantly reduces future costs. Application of security by design can range from continuous testing and permanently monitoring software development to simultaneously and automatically identifying poor coding styles that potentially jeopardize software security.

FROM PREVENT & PROTECT TO PREDICT, MONITOR & RESPOND

Today's cyber threats demand an active approach to security. Instead of building defenses and waiting for something to happen, the focus should be on predicting, monitoring, and responding to attacks. Before, during, and after. The following recommendations enable firms to be more aware of and responsive to Digital Trust & Security threats.

Implement an Effective Security Operations Center

TECHNICAL

A Security Operations Center (SOC), equipped with Security Information and Event Management (SIEM) software, enables comprehensive analysis of security events to detect threats and anomalies. While the primary responsibilities of the operations teams are SOC/SIEM administration services as well as threat monitoring and threat response, an emergency response team takes over in case an incident is detected. They will immediately take the necessary actions to prevent further damage.

Use Digital Analytics to Identify Intrusions and to Predict Future Incidents

TECHNICAL

A complete prevention of intrusions is impossible, so it is important to be able to identify the advanced persistent threats that have breached the system as quickly as possible. Digital forensics, incorporated in a SOC, help to locate such breaches through extensive data analytics. Human experts and big data algorithms have proven to be an especially successful combination in this context. Artificial intelligence-based software can go one step further by helping to predict future incidents automatically.

Maximize Resilience

ORGANIZATIONAL TECHNICAL

As attacks will happen and they will be successful sooner or later, it is necessary to learn to live with this permanent threat. A company that maximizes its resilience, i.e., its ability to deal with cyber-attacks and their consequences, increases its chances to prevent disastrous attacks. Backup and recovery strategies are fundamental to be able to restore data in case of an incident. Isolating data crown jewels from the internet in case of an attack can help dispel disaster. Moreover, sound business continuity plans and incident response teams are crucial to be able to resume business operations as quickly as possible.

FROM MANUAL TO AUTOMATIC & INTELLIGENT EXECUTION

Monitoring and responding to Digital Trust & Security threats and breaches often requires significant manpower. In addition to the associated costs involved with this, results are that Digital Trust & Security experts being tied up in these 'clean up' activities, when their expertise is better used to complement new projects and innovations. This can be achieved by changing the company mindset from manual to automatic.

Automate as Much Digital Trust & Security as Possible

By automating as many Digital Trust & Security systems and processes as possible, the workload of security specialists is reduced, and they gain capacity to bring value to other parts of the company. The following are some of the processes that can be automated:

- Incident classification: a Security Operations Centre receives large amounts of Digital Trust & Security notifications every day. Filtering and prioritizing alerts to find the ones that need specialist attention most urgently often takes a lot of time.
- Patch management: automatic software updates to patch vulnerabilities not only saves up specialists' time, it also significantly reduces the window of opportunity for attackers.
- Creating and testing backups: making sure that essential documents are backed up as well as testing whether backups that have been made are not corrupted can take a lot of time.
- Fine-tuning firewall configuration: firewalls need to be adjusted to fit the needs of the company as well as to cope with ever-changing Digital Trust & Security threats. In addition to reducing the window of opportunity for attackers and saving time, by automating this process, employees may experience fewer service disruptions.

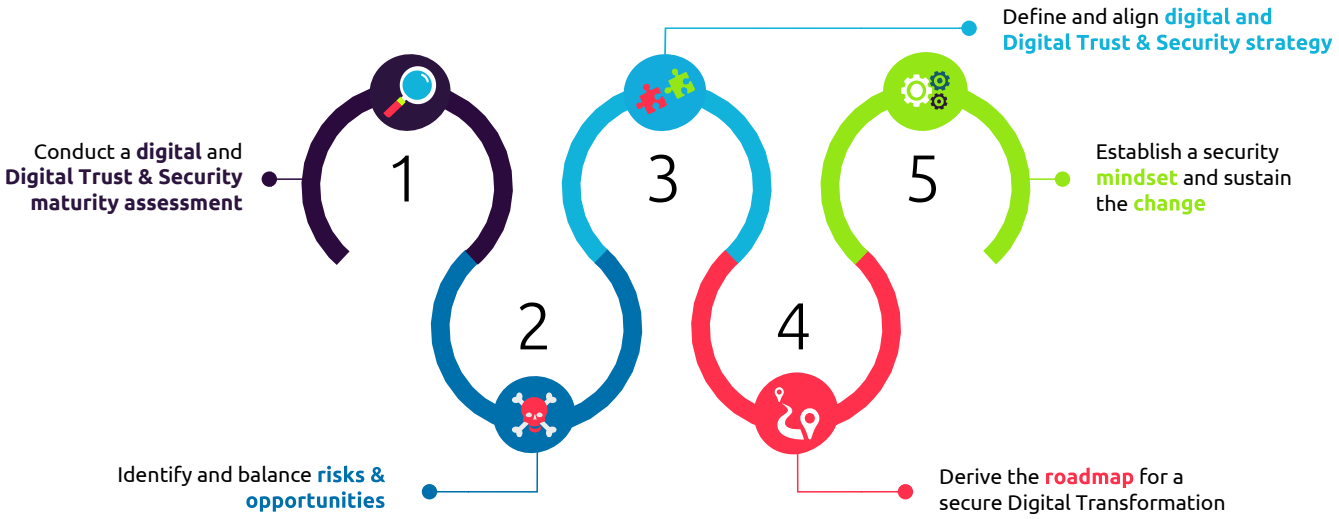
Employ Advanced Intrusion Response Systems

AI-powered IDPS (Intrusion Detection and Prevention System) applications can learn to recognize threats and breaches that they were not originally designed to detect. These advanced applications can be programmed to respond quickly and appropriately to such incidents with several new means at their disposal. For example, they can be set to back-hack attackers by letting them steal documents that are fitted with tracking systems, or they can be set with obfuscation techniques that simulate gigantic infrastructures the second an attacker gains access to the network, reducing the chance they find the locations they intended to. These measures are advanced and require specific skills to implement properly, but can potentially pay for themselves as a result of the damage they prevent.

4. NEXT STEPS

Those companies that incorporate Digital Trust & Security into their Digital Transformation will have a higher chance of successfully realizing the benefits of both. Managing this balance well results in growth, improved resilience, and cost reduction. To achieve this, organizations must change their mindset from deterrence and protection to prevention and full resilience. At the same time, the impact of a breach should be actively minimized and compliance with new data protection regulations needs to be ensured. In the previous sections, recommendations were discussed to help organizations transition into the paradigms that are necessary to transform digitally while staying ahead of Digital Trust & Security threats. The following five recommendations are the first practical steps organizations should take to secure their Digital Transformation while working on their paradigm transition.

Figure 5: Digital Trust & Security Approach



1. CONDUCT A DIGITAL AND DIGITAL TRUST & SECURITY MATURITY ASSESSMENT

An assessment provides a comprehensive overview of the organization's current Digital as well as Digital Trust & Security posture. For an organization, it is important to identify maturity gaps to prioritize future measures properly. Benchmarking the results against peer companies gives insight into what areas of investment should be prioritized.

2. IDENTIFY AND BALANCE RISKS & OPPORTUNITIES

With the assessment results on hand, it is essential to develop an understanding of the way the world is changing. Continuously monitoring Digital Transformation trends and identifying opportunities and resulting risks helps organizations to understand what changes to adapt to, and how. It is important to find the right balance between these opportunities and threats that fits the firm's needs.

3. DEFINE AND ALIGN DIGITAL AND DIGITAL TRUST & SECURITY STRATEGY

Once maturity, risks, opportunities, and necessary changes are clear, they must be captured in the company strategy. In the formulation of the company strategy, Digital Trust & Security should be one of the cornerstones that is deeply embedded in the organizational model as a sustainable business enabler.

4. DERIVE THE ROADMAP FOR A SECURE DIGITAL TRANSFORMATION

With the new strategy and a comprehensive overview of new opportunities and threats at hand, areas of the business can be identified, ranked, and prioritized based on their transformation complexity and necessity. Based on these priorities, a roadmap for the organization's Digital Transformation should be created. Each of the implementation steps and milestones on the roadmap should include the associated Digital Trust & Security risks and measures to address them.

5. ESTABLISH A SECURITY MINDSET AND SUSTAIN THE CHANGE

While implementing the planned steps has high priority, organizations must continuously adapt their roadmap to new trends, opportunities, risks and threats that are brought forth by the ongoing Digital Transformation. Setting up a Security Operations Center (SOC) is essential to ensure that Digital Trust & Security definitions, policies, and measures are integrated in every step along the way set out on the roadmap. Additionally, it is also necessary to train employees to keep them up to speed on the latest best practices and pitfalls regarding Digital Trust & Security. Comprehensive KPI tracking gives the organization insight into how well the implementation is going and what areas need more attention.

With these ongoing efforts, companies can make sure to combine the benefits and opportunities of the Digital Transformation with a well-grounded Digital Trust & Security approach. A secure Digital Transformation approach is the core of sustainable success.

5. CONTACTS

Dr. Paul Lokuciejewski
Principal
+49 151 4025 0855
paul.lokuciejewski@capgemini.com

Sebastian Heierhoff
Manager
+ 49 151 4025 0133
sebastian.heierhoff@capgemini.com

Additional Authors

- Anton Haberl, Senior Manager
- Dr. Stephan Schlagkamp, Senior Consultant
- Sarah Schuckert, Consultant

About
Capgemini Invent

As the digital innovation, consulting and transformation brand of the Capgemini Group, Capgemini Invent helps CxOs envision and build what's next for their organizations. Located in more than 30 offices and 22 creative studios around the world, its 6,000+ strong team combines strategy, technology, data science and creative design with deep industry expertise and insights, to develop new digital solutions and business models of the future.

Capgemini Invent is an integral part of Capgemini, a global leader in consulting, technology services and digital transformation. The Group is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of over 200,000 team members in more than 40 countries. The Group reported 2018 global revenues of EUR 13.2 billion.

Visit us at

www.capgemini.com/invent

People matter, results count

Capgemini invent