WHITE PAPER

Cyber Security Transformation

How to deliver the new cyber security paradigm

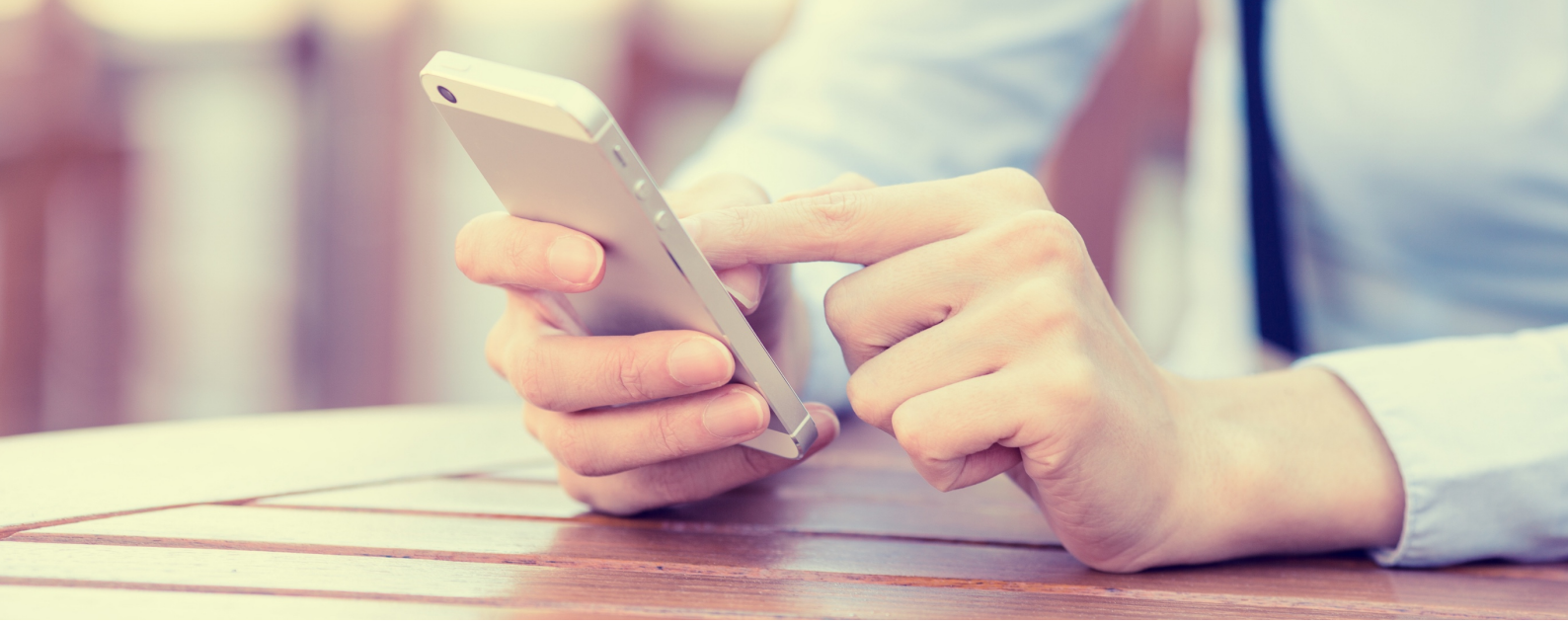
Author: Mathieu Poujol, Head of Cyber Security

July 2018

Infosys

PAC
A CXP GROUP COMPANY

Summary



DIGITAL TRANSFORMATION

IT AT THE CORE OF THE VALUE CHAIN

Our world is becoming increasingly digitalized, and most organizations are facing new challenges in terms of speed, innovation, agility, and of course performance in an ecosystem-based model. To meet these challenges, they have to transform themselves by integrating the digital value chain. Digitalization has become the natural, imperative evolution of these organizations because, as in any revolution, the players' positions are changing, with those who digitalize standing a better chance of winning. Against the backdrop of this transformation, organizations have become more open, with innovation being once again the prime goal for most of them.

To achieve this digital transformation, organizations are increasingly focusing on information and communication technology (ICT). As a result, ICT has become ubiquitous in companies, from the business unit level to the ecosystem level, generating an ever-increasing added value, and often being the main source of innovation. At the heart of this third industrial revolution, data is the energy and cloud-based systems are the factories.

65%

of IT decision-makers think that digital transformation is important or very important in their IT agenda

CxO Survey 2018, PAC

OPENNESS, SPEED, AND CHANGE

With the start of this revolution, the Earth has been getting smaller, with markets expanding from local to global while opening up at the same time. This has propelled innovation, which today very quickly reaches a global scale, as well as business-related change and transformation.

Businesses are therefore seeking to make their organizations more agile and innovative, and are opening their ecosystems more and more to partners, suppliers, and customers. This requires greater flexibility of computer systems, which explains the increasing use of cloud computing (related to applications or infrastructure) as an architecture and as a service. As digital transformation aims to break

up the silos separating business, development, and production, it opens up the IT, linking new cloud-based systems to legacy systems.

These hybrid architectures, which are therefore the reference architectures of digital transformation, need cyber security to live up to their potential. Our digital business models are becoming global, based on ecosystems and innovation, with silos being broken up, and speed and agility being key attributes. The strengths of this model are its openness, speed, and ability to change.

The key strengths of the digital model are openness, speed, and the ability to change

CYBER SECURITY TRANSFORMATION

MORE AND INCREASINGLY DANGEROUS ATTACKS

Digital transformation has opened up economies, businesses, and information systems, making them more vulnerable and exposing them to more attacks. This situation endangers digital transformation as well as the very existence of the enterprises that are transforming. Cyber security is a key catalyst for digital transformation.

We could fill pages with statistics on cyber-attacks, but the conclusion is very simple: in our digital world, cyber security is at least as important as physical security. Security has always been an essential component of any economic system, because – just like with countries – the safer economies are, the more activities develop. The same applies to digital transformation.

What is more, the impact of cyber-attacks is no longer virtual, but affects the top and the bottom line and can even cause physical damage. There are many examples and not a week goes by without an attack being reported. They can have various different goals, mainly data theft, data loss, or the disruption of activities (online services or physical processes), with more and more serious effects.

Governments, businesses, and individuals have become aware of these impacts, which may damage a company's reputation and competitiveness or even lead to bankruptcy.

As a result, regulations have tightened for specific industries (Basel III, IATA etc.) but also at regional (EU GDPR, NIS) or national levels. Organizations that do not abide by these regulations will have to pay fines, which in the case of European directives, for instance, may amount to up to 4% of annual turnover.

78%

of IT decision-makers think cyber security is important or very important in their IT agenda

CxO Survey 2018, PAC

FULL USAGE OF THE DIGITAL WEAPONS

Pirates and corsairs (state-sponsored pirates) of the Internet have transformed themselves much faster than companies and authorities. These attackers are using the capabilities of digital technologies to launch and coordinate an increasing number of mutant attacks with

ever-growing firepower. These quasi-industrial organizations are based on cloud architectures, whose capabilities they make maximum use of. They mostly employ purpose-built solutions that are very lightweight as they heavily rely on external cloud capacities.

The distribution and globalization of the digital world is highly conducive to their activities, allowing them to find and hire the best technologies and experts, and to combine them in a virtual cloud infrastructure to wreak havoc across the globe. This type of infrastructure offers them considerable protection from law enforcement, while punishment is very light compared to the potentially huge gains. They use cloud-based technologies such as cryptocurrencies to get paid and to launder their money.

The mass of information, some of it personal (from social media, for example), that is available on the Internet is a gold mine for the hackers, allowing them to better exploit their targets' vulnerabilities.

Businesses today acknowledge that cyber security is a key enabler of digital transformation. They have therefore begun to invest in the topic to ensure the success of their initiatives. And while the quantity of investments is important, it is their quality that is critical as there are ever more attackers and fewer defenders.

Businesses today acknowledge that cyber security is a key enabler of digital transformation

Expert view:

"People ask me all the time, 'What keeps you up at night?' And I say, 'Spicy Mexican food, weapons of mass destruction, and cyber-attacks.'

Dutch Ruppersberger, US Representative, 2016

PARADIGM SHIFT IN CYBER SECURITY

The digital world is characterized by its need for agility, coupled with widely distributed and open systems – and most organizations have to adopt this model. This is the opposite of the fortress it should be to facilitate securing IT systems. Moreover, the significance of IT to all aspects of our business and private activities makes the human factor an even more dangerous vulnerability. It is very important to tackle these issues in order to be able to fully exploit all the benefits of digital transformation. For this purpose, we need a new paradigm as traditional security is too limited.

HOLISTIC APPROACH

Digital systems are full-stack, hybrid, and interconnected systems spanning all IT layers, from the network to the business, and linked to numerous other systems and third-party IT and IT services providers. This vertical and horizontal complexity is a key source of vulnerability for nearly all organizations since it makes it difficult to secure such heterogeneous systems, leaving some unprotected weak spots. This is precisely where hackers will attack.

Organizations must adopt a holistic approach to cyber security, based on the classification of their data and processes according to criticality, which goes well beyond traditional perimeter security. All layers of IT have to be secured and controlled using a "defense in depth" approach to cyber security, with cyber security tightening when it comes to the key parts of the business while still permitting the business to run well.

$57-109 billion

costs related to cyber security incidents for the US economy in 2016

The Council of Economic Advisers, White House, US Government, 2018

VISIBILITY

To realize a holistic approach to cyber security, organizations require visibility of the complex business partner network and the complex hybrid systems. This holistic visibility is achieved through full collaboration with business partners and most importantly with all the IT stakeholders within the company, which enables you to know and manage the security of the different IT assets in the organization. You cannot protect what you do not know. Another aspect is the ability to gain a complete view of vulnerabilities and threats in real time and correlate and analyze them. Here a security operations center (SOC) is all but mandatory.

CLOUD AND AI

At the core of this new paradigm is the combination of big data and artificial intelligence powered by cloud computing. Artificial intelligence is not a novelty; it has been used for decades in very specific, often military systems. In the past, though, its algorithms required a lot of data and computing power, so AI could not be used in real time at an affordable price. Cloud-powered big data, together with the explosion of data generated, have solved these issues. As with retail systems, where big data can detect hidden patterns that permit to sell more and better, cyber security-oriented systems can use the same approach to reduce vulnerabilities, monitor systems, and prevent and fend off cyber-attacks.

The new cyber security paradigm: holistic approach, visibility, cloud, and AI

Expert view:

"We are responsible for directing citywide cyber defense and incident response and mitigating cyber threats. How do you do that? You need to be able to have technology that goes out there, gives you visibility, and gives you technical controls over the various systems that could be impacted in a cyber event."

Geoff Brown, NYC CIO 2017

THE ISSUE OF RESOURCES

TALENT SCARCITY

Cyber security operations heavily rely on human resources. A growing number of staff is needed, and they have to be available around the clock; for example, a standard 365x7x24 SOC needs at least 20 people. Growing threats and vulnerabilities as well as compliance issues across the globe have created a huge need for rare cyber security experts. Besides having cyber security expertise in specific fields, they increasingly also have to understand other aspects of IT that cyber security depends on to be effective.

2 million
cyber security professionals will be lacking globally by 2020

ISACA, 2017

Military images are frequently used for cyber security, and just like any war, cyber security needs soldiers. Modern armies, however, no longer need only standard soldiers, but also well-trained specialists and veterans. Likewise, in the cyber security space, you also need those profiles, and they are not easy to recruit and keep in your organization. In addition, the education systems do not train enough specialists, and those specialists have to gain some "battlefield experience" to be efficient.

In any market economy, what is rare is expensive, and this is clearly the case with cyber security experts, which is why their salaries are becoming a huge burden. This lack of talent has been hampering many cyber security projects.

RIGHT-SHORING

Early on, international businesses, IT services companies, and software suppliers started to look for talent beyond the main business hubs. There are several ways to hunt for rare talent:

- Local service centers have been established as part of a "country shore" model, e.g. in France, where resources are less expensive and more loyal to their company when outside of the Paris region.
- Similarly, immigration has become a well-developed strategy for multinational companies in places such as the Middle East, Germany, or the USA.
- Nearshore and offshore options have been growing fast, especially for global and highly standardized workloads.

In many cases, the best way is to combine the three methods above when hunting for talent and to use outsourcing, as the mutualization of these rare resources is imperative. In cyber security, more than in any other market segment, sharing and learning from an outsourcer is important. This is why right-shoring is a key asset of any cyber security practice: a mix of local, business-oriented specialists, along with a continental service center; global coverage and offshore capacities for the most standardized workloads. When deploying right-shoring, it is very important to pay attention to compliance issues.

All this is not sufficient, though. Just like the Internet pirates, companies should make better use of digital technologies. Cloud-based services and technologies are flexible, scalable, optimized, and automated, and thus well-adapted to the digital economy and to the lack of cyber security talent.

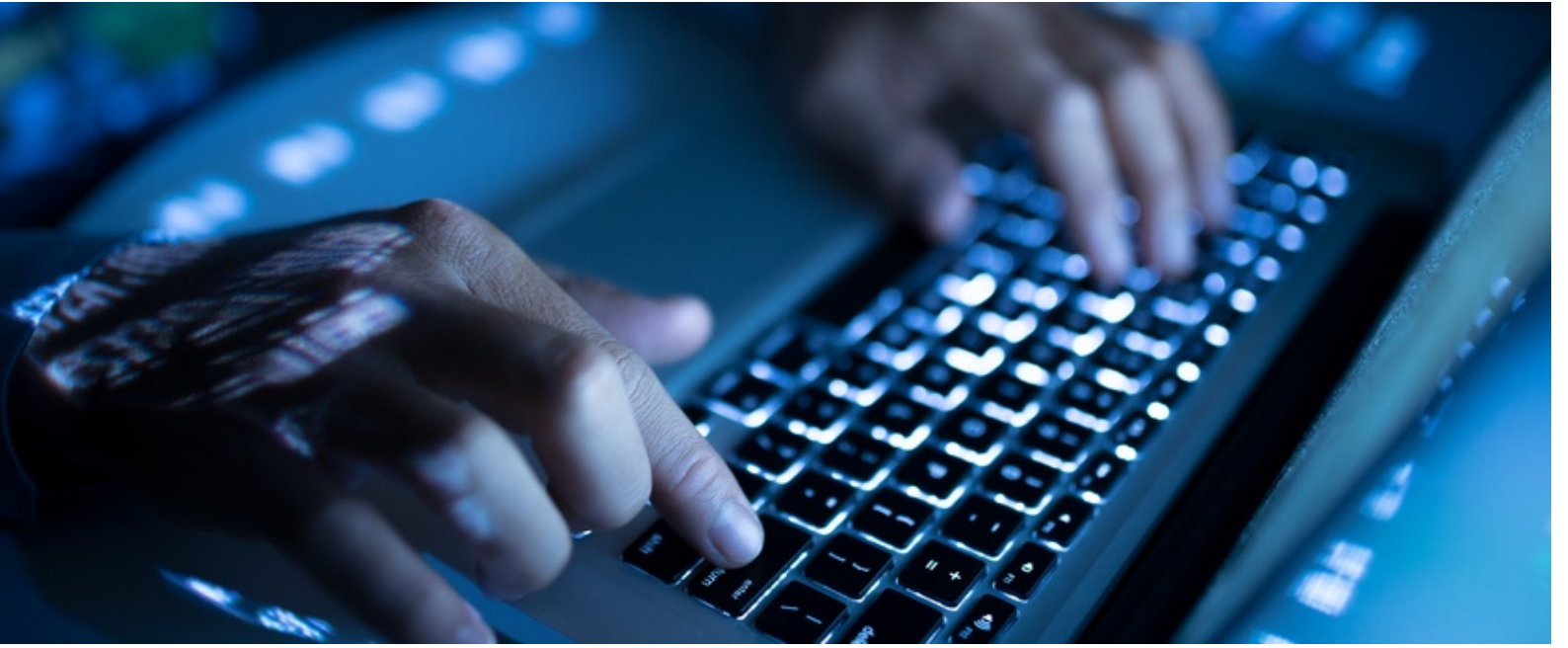
Cyber security outsourcing services represented

€9.5 billion

globally in 2017

SITSI cyber security figures, PAC, 2018

Human resources are at the core of cyber security issues



AUTOMATE INTELLIGENTLY

OPTIMIZE YOUR INVESTMENTS

Automation always was the cornerstone of the previous industrial revolutions, viewing as it optimized resource utilization. This is also the case with the current digital revolution, and it is even more significant in a tight market such as cyber security.

Similar to the digital business, cyber security is all about speed – preventing, stopping, and quickly fixing cyber threats. Automation frees up human resources for the most important tasks, where they can have a maximum impact on the business. Automation does not replace the analysts but helps them focus on areas where they can generate the biggest added value and where human decisions are needed, while automated systems do all the lesser work. This is why robotic process automation (RPA) is so important in cyber security, as it makes it possible to perform tasks more quickly with fewer resources. Additionally, automation leads to repeatable processes that can be measured and optimized, resulting in better quality. Automation is not only relevant for cyber security, but also for the related segments of IT asset management, IT service management, and patching.

Expert view:
"Productivity and quality gains are huge when you combine RPA and human talent."

Roberto Mancone, MD, Global Head, Disruptive Technologies & Solutions, Deutsche Bank, 2017

PROTECT ALL YOUR ASSETS

Naturally, the technological foundations of automated systems are cloud-based, as cloud technologies are already optimized and perfectly aligned with cyber security issues.

Cloud computing architectures permit an easier deployment of cyber security over all types of IT systems, devices, and business activities. All new concepts are cloud-based, such as IoT or mobility, and cloud technologies are the best choice for protecting cloud-based systems.

Cloud computing also offers a much more efficient way of using outsourcing, thanks to its flexibility and also its cost optimization. For example, cloud-based SOCs allow many SMBs and subcontractors of

large enterprises to be better protected. Cloud computing is a way to make optimum use of the pool of human resources with security expertise. Similarly, it is very hard to secure all data generated or federated ID and access management within large multinationals without cloud delivery models. With the cloud you can protect all your assets, even the most distributed ones.

DELIVER THE NEW CYBER SECURITY PARADIGM

Moreover, without the capacities of cloud computing and automation there will be no new cyber security paradigm: automated cloud environments power the computing and storage needs of AI boosted by big data analytics.

Finally, to deliver this new paradigm, to use more automation, and to fully exploit the potential of cloud technologies, you have to collaborate with a partner that specializes in these new ways to deliver cyber security. Best practices are essential in this fast-moving field of cutting-edge technology, providing support both in the project phases and with operations, not to mention the delivery of additional human resources through cloud services.

An IT services partner is essential for achieving a suitable level of cyber security.

Without the capacities of cloud computing and automation, there will be no new cyber security paradigm

Expert view:
"AI has a huge impact on cyber security."

Guillaume Poupard, General Manager, ANSSI, the National Cybersecurity Agency of France, 2017

INFOSYS' RESPONSE TO THESE CHALLENGES

INFOSYS' VISION

Constantly innovating hackers are driving CIOs and CISOs to react to each new cyber threat by simply bolting on more and more point solutions. The list is endless: endpoint controls, application firewalls, protection against data loss, anomaly detectors, and so on. Often, the result is a patchwork of point solutions that not only do not work well together, but are inadequate to protect against evolving threats that are now spread across an attack surface with thousands of potential entry points, including those created by smart phones and Internet of Things (IoT) devices. It is little wonder that they find themselves spending valuable time managing 'reactive security' rather than driving innovation. They want to secure their digitized core, front ends, and ecosystem so that they can run their business and enable a digital journey at scale.

The need of the hour is for flexible and adaptive security solutions, delivered in an integrated package that can be consumed 'as-a-service' through a simple engagement model with commercial flexibility. This would make it possible to not only prioritize rapid remediation, but also plan for anticipatory protection, without the huge operational and cost overheads required to manage a fragmented landscape with point solutions pieced together. The CIO and CISO can, instead, focus precious time and resources on accelerating the enterprise's digital innovation agenda.

Infosys in 2017:

- $10 billion+ in revenue
- 200,000+ employees
- 45+ country offices

Infosys, 2018

WHY INFOSYS?

Infosys helps CISOs create the productivity savings they need to focus on the innovations that help drive their agile digital business, while they manage the risks of an increasingly sophisticated threat environment. Infosys offers security as a service, through the Infosys Cyber Security Platform, built with AI-driven automation at its core, to help CIOs and CISOs transition from a fragmented and reactive approach to a managed security services model with a customized roadmap. This guarantees AI-driven efficiencies, lower TCO, and a robust incident management process every single day. It brings together an optimized tool suite, a proactive approach to security, and strong predictive capabilities needed to protect against advanced threats.

Infosys services are differentiated by:

- Infosys Cyber Security Platform that is a scalable, managed detection and automated incident response platform that enables integrated incident monitoring, orchestration, and automated response for protection against cyber-attacks. The platform provides a unified view of the security posture across the IT infrastructure, leveraging analytics and automation, with agility, scalability, adaptability, and ability to integrate with diverse work environments, while maintaining a consistent level of service.
- Infosys Security Operations Centers (24x7 SOCs), already operational in Bangalore, Hyderabad, and Pune, that bring together best-in-class skills and a constantly updated solutions suite along with managed services for noiseless security operations delivered round-the-clockthrough a world-class, network of interconnected, global facilities.
- Infosys Engineering and Research Labs that give their clients access to advanced threat hunting capabilities and the latest in technology innovations for cyber security. This is Infosys' investment in continuously improving its core services portfolio, expanding its offerings into new potential threats, and leveraging our innovation ecosystem to co-create solutions that can deepen the value Infosys delivers.

90%

manual checking efforts eliminated on average for Infosys' cyber security clients

Infosys, 2018

Integrated Cyber Security Platform

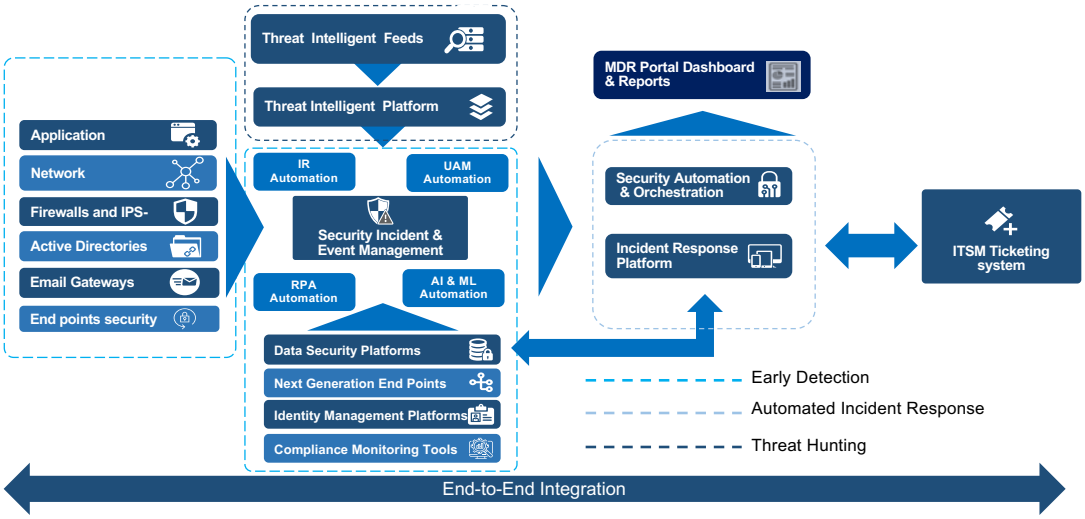


Fig. 1: Infosys' cyber security offer

THE VALUE INFOSYS DELIVERS TO CLIENTS

For most enterprises, application security remains an afterthought until a breach happens. And Infosys client, a large device manufacturer, was no exception. When one of their strategic web applications was hacked, they approached Infosys to put in place an app security testing program with one goal – to reduce the chances of similar breaches in future.

Using a wide range of tools and services, Infosys developed a testing program that could scan, detect, and flag all possible issues in thecode. Infosys soon realized that this process threw up a lot of false alarms. So Infosys went a step further and developed a tool to filter out false alarms and allow the team to focus on important weaknesses. What evolved was a stronger, more robust security platform that could easily be scaled as per the needs of its client's application landscape.

The result?

- 90% manual checking effort eliminated
- 85% increased coverage
- 0 defects in production

THE ROAD AHEAD FOR INFOSYS

- Establish an end-to-end security program for its clients and employ integrated security capabilities in the areas of GRC, Adaptive
- Authentication & Access Management, Data Security, Threat Management, and Cloud & Mobile Security.
- Build best-in-class SOCs with behavior-based technologies and advanced analytics to enable proactive defense and predictive cyber threat intelligence.
- Use cloud engagement models, productized solutions, and an as-a-service model in a partner environment to provide comprehensive security solutions.
- Set up a strong in-house security center of excellence and create advanced training programs in collaboration with Purdue University and others, for both fresh graduates and lateral hires.
- Build delivery excellence through automation and non-linear engagement models.• Build delivery excellence through automation and non-linear engagement models.

85%

increased coverage on average for Infosys cyber security clients

Infosys, 2018

ABOUT INFOSYS

Infosys is a global leader in next-generation digital services and consulting. We enable clients in 45 countries to navigate their digital transformation. With over three decades of experience in managing the systems and workings of global enterprises, we expertly steer our clients through their digital journey. We do it by enabling the enterprise with an AI-powered core that helps prioritize the execution of change. We also empower the business with agile digital at scale to deliver unprecedented levels of performance and customer delight. Our always-on learning agenda drives their continuous improvement through building and transferring digital skills, expertise, and ideas from our innovation ecosystem.

Infosys
Corporate Headquarters
Electronics City,
Hosur Road
Bengaluru 560 100

Phone: +91 80 2852 0261
Fax: +91 80 2852 0362
www.infosys.com

ABOUT PAC

Founded in 1976, Pierre Audoin Consultants (PAC) is part of CXP Group, the leading independent European research and consulting firm for the software, IT services, and digital transformation industry.

CXP Group offers its customers comprehensive support services for the evaluation, selection, and optimization of their software solutions and for the evaluation and selection of IT services providers, and accompanies them in optimizing their sourcing and investment strategies. As such, CXP Group supports ICT decision-makers in their digital transformation journey.

Further, CXP Group assists software and IT services providers in optimizing their strategies and go-to-market approaches with quantitative and qualitative analyses as well as consulting services. Public organizations and institutions equally base the development of their IT policies on our reports.

Capitalizing on 40 years of experience, based in 8 countries (with 17 offices worldwide) and with 140 employees, CXP Group provides its expertise every year to more than 1,500 ICT decision-makers and the operational divisions of large enterprises as well as mid-market companies and their providers. CXP Group consists of three branches: Le CXP, BARC (Business Application Research Center), and Pierre Audoin Consultants (PAC).

For more information please visit: www.pac-online.com

PAC's latest news: www.pac-online.com/blog

Follow us on Twitter: @CXPgroup

A CXP GROUP COMPANY

PAC - CXP Group
8, avenue des ternes
75017 Paris

Tel. : +33 (0)1 53 05 05 53
info-france@pac-online.com
www.pac-online.com

DISCLAIMER, USAGE RIGHTS, INDEPENDENCE, AND DATA PROTECTION

The creation and distribution of this study was supported by Infosys.

For more information, please visit www.pac-online.com.

Disclaimer

The contents of this study were compiled with the greatest possible care. However, no liability for their accuracy can be assumed. Analyses and evaluations reflect the state of our knowledge in April 2018 and may change at any time. This applies, but not exclusively, to statements made about the future. Names and designations that appear in this study may be registered trademarks.

Usage rights

Independence and data protection

This study was produced by Pierre Audoin Consultants (PAC). The sponsors had no influence over the analysis of the data and the production of the study.

The participants in the study were assured that the information they provided would be treated confidentially. No statement enables conclusions to be drawn about individual companies, and no individual survey data was passed to the sponsors or other third parties. All participants in the study were selected at random. There is no connection between the production of the study and any commercial relationship between the respondents and the sponsors of this study.

A CXP GROUP COMPANY