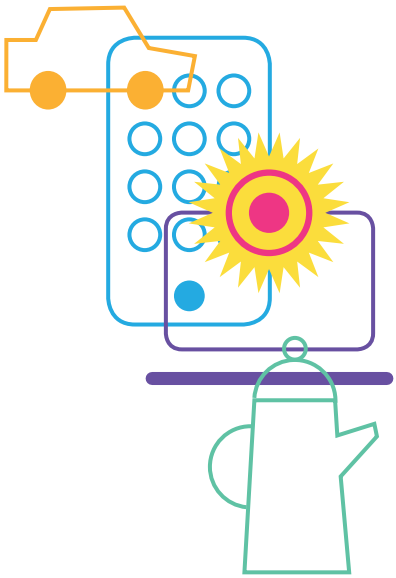
Proactive Protection: How Companies Can Secure Customer Data in a Hyper-Connected World

Today, digital customer experience transformations are mandatory to stay ahead in business, not optional. Customers are demanding cutting-edge digital experiences, delivered on every channel, via every device, anytime and anywhere they desire. To satisfy these customers, companies are transforming their digital platforms, processes, and practices, leveraging new technologies, such as machine learning and artificial intelligence, and implementing Lean approaches and Design Thinking.

But although digital transformations are required, they are not risk free. These transformational projects generate a dizzying array of new cybersecurity risks. New digital processes generate mountains of customer data. Much of this data is stored inside the organization; some is shared with business partners. More data, stored in multiple places, provides a bigger, softer target for external hackers and internal bad actors.

The stakes are high. Any breach or leak of customer data can cost significant money to address. It also can incur the wrath of regulators and do serious damage to a company's reputation.

Consequently, any company embarking on the digital transformation of their customer experience must make cybersecurity an integral part of their organizational culture.



Every New Touchpoint Brings New Risks

Right now, companies are supplying their customers with billions of digital apps, devices, and smart, internet-connected products—kitchen appliances, medical devices, cars—that, together, comprise the Internet of Things (IoT). And every new app, device, and gizmo accesses and generates data.

Traditionally, companies stored data—both customer and transactional—in a centralized and controlled manner, within the company's four walls, in databases that were guarded and protected. Today, that kind of control is impossible, and not even desirable. Data is generated everywhere, all the time, flowing into the organization from millions of distributed devices in the hands of customers and partners, not to mention from sensors critical to business operations in sectors ranging from retail to telecommunications to manufacturing.

These connected devices are proliferating at an astonishing rate. According to Gartner, there will be 20.4 billion connected devices in use worldwide by 2020, more than double the number deployed at the end of 2017.[1]

Each of these connected digital devices serves as a touchpoint through which companies and customers interact for purposes of marketing, sales, customer service, payments and more. And each of these billions of touchpoints represents a potential point of attack that people with bad intentions—either criminal hackers or disgruntled employees—can exploit. Data theft or misuse not only constitutes a reputational and financial risk to corporations but could have disruptive impact on customers' lives. For example:

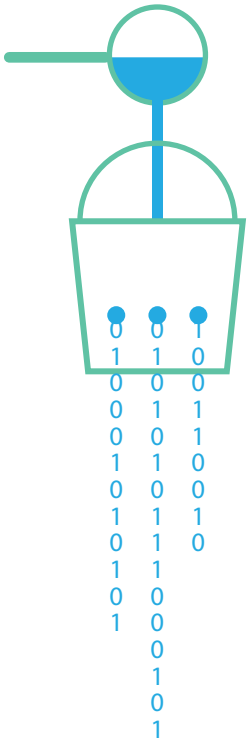
- In 2017, *Wired* warned that connected medical equipment—from sensors and monitors to implantable devices like pacemakers and insulin pumps—were all vulnerable to hack attacks. Once they gain access, hackers could steal medical records, execute ransomware attacks or even cause a device to malfunction so that, for example, a patient might receive a fatal overdose of insulin.[2]

[1] "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent from 2016," press release, February 7, 2017, accessed at: https://www.gartner.com/newsroom/id/3598917

[2] "Medical Devices Are The Next Security Nightmare," Wired, March 2, 2017, accessed at: https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

In the absence of a new strategy for cybersecurity, simply increasing the size of the cybersecurity spend will not be sufficient to cope with the magnitude of the threat at hand.

- White hat hackers publicized the fact in 2017 that they had been able to access the infotainment system—including microphone, navigation system and speakers—on certain Volkswagen and Audi models.[3] As automakers move forward with plans for hands-free driving, and eventually fully autonomous vehicles, the health and safety implications of hack attacks on connected cars becomes realistically dire.
- More and more consumers are stocking their homes with IoT devices including baby monitors, security cameras, doorbells and thermostats. But researchers at Israel's Ben-Gurion University found that the security protocols on such off-the-shelf IoT devices were easily breached.[4] Indeed, there are anecdotal reports of malevolent strangers hacking into baby monitors to shout insults at children and their parents, play music or hijack control of the camera.[5]
- At the 2017 Mobile World Congress Americas, an IoT Security expert conducted a live hack attack on a fictional home with multiple IoT devices, quickly taking control of an Amazon Echo, IP camera, smart alarm and smart lock to gain physical access to the home.[6] This scenario is especially troubling given Berg Insight's prediction that more than half of all homes in North America will become smart homes by the year 2021.[7]



Pouring Money into the Wrong Buckets

Companies know that cybersecurity risks are rising; they want to protect themselves and their customers, so they are ramping up their cybersecurity spending. IDC predicts that spending on security-related hardware, software and services will reach $91.4 billion worldwide in 2018, a 10.2 percent increase over 2017.[8] Spending on cybersecurity will continue to soar over the next three years, especially in the telecommunications sector where IDC projects a 13% CAGR in cybersecurity investments.

But are companies making the right sort of cybersecurity investments? We believe that in the absence of a new strategy for cybersecurity, simply increasing the size of the cybersecurity spend will not be sufficient to cope with the magnitude of the threat at hand.

[3] "VW-Audi security: Multiple infotainment flaws could give attackers remote access," ZDNet, May 1, 2018, accessed at: https://www.zdnet.com/article/vw-audi-security-multiple-infotainment-flaws-could-give-attackers-remote-access/

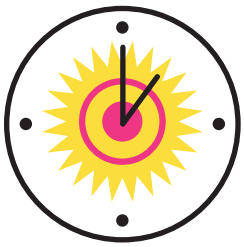
[4] "Off-the-shelf smart devices found easy to hack," American Associates, Ben-Gurion University of the Negev via EurekAlert!, March 13, 2018, accessed at https://www.eurekalert.org/pub_releases/2018-03/aabu-osd031218.php.

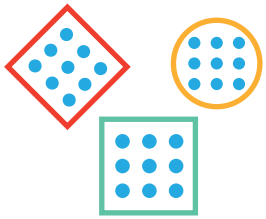
[5] "7 Creepy Baby Monitor Stories That Will Terrify All Parents," Buzzfeed, July 24, 2015, accessed at https://www.buzzfeed.com/craigsilverman/creeps-hack-baby-monitors-and-say-terrifying-thing?utm_term=.lv5x8xWo0#.gpokGkDLv

[6] "This Company Staged A Hack With Multiple Devices To Show Your Home's Vulnerability," Forbes, September 19, 2017, accessed at https://www.forbes.com/sites/jenniferhicks/2017/09/19/this-company-staged-a-hack-with-multiple-devices-to-show-your-homes-vulnerablity/#4ac5f4975322

[7] "73 Million Smart Homes In North America Projected," MediaPost, July 13, 2017, accessed https://www.mediapost.com/publications/article/304304/73-million-smart-homes-in-north-america-projected.html

[8] "Worldwide Spending on Security Solutions Forecast to Reach $91 Billion in 2018, According to a New IDC Spending Guide," press release, March 27, 2018, accessed at: https://www.idc.com/getdoc.jsp?containerId=prUS43691018.





Here are four reasons why companies cannot rely on more of the same when it comes to cybersecurity:

1. **Reactive solutions are no longer sufficient.** Cybersecurity practitioners have traditionally focused on detecting problems and then reacting to them with countermeasures.

   This strategy no longer suffices in 2018, as hackers can now do more damage more quickly and have become more adept at hiding their tracks.

2. **Data is everywhere, and it is largely unstructured.** Legacy cybersecurity models focused on protecting structured data that lived within a corporate database. But now data is unstructured, coming into the enterprise a wide variety of formats, from word files and spreadsheets to images, videos, audio and more. In addition, critical corporate data now resides everywhere, in the cloud and on billions of devices scattered across the planet. (According to Gartner, there will be 20.4 billion internet-connect "things" by 2020.[9]) One cannot erect a firewall around every individual with a smartphone or laptop or digital assistant everywhere in the world.

3. **Companies no longer own the devices that hold their data.** Before the IoT, cybersecurity teams could focus on hardening defenses around a select group of internal IT systems, data centers, and networks. But today there are billions of IoT devices, each a potential entry point for an attacker. For example, Target suffered a damaging breach after hackers gained access to its payment systems and stole login credentials through an internet-connected HVAC system.[10]

   For a hacker, any IoT device could be the back door to the larger system. In a hospital, it could be an internet-connected MRI machine or CT scanner. In a household, it could be an appliance or a digital assistant. Recently, researchers have demonstrated their ability to eavesdrop and record voices of people using Amazon's popular Alexa-enabled Echo speaker.[11]

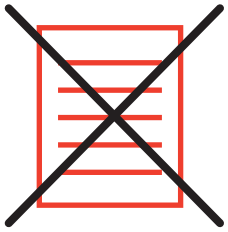
   And it's not just devices. Even browsers or apps can give hackers a way into the enterprise. Today, it is no longer possible to draw a bright line around where the corporate network begins or ends.

Proliferation of data centers both magnifies overhead costs and increases the complexity of blocking hackers from gaining access to steal data or otherwise wreak havoc.

[9] "Gartner Says 8.4 Billion Connect 'Things' Will Be in Use in 2017," February 7, 2017, accessed at https://www.gartner.com/newsroom/id/3598917

[10] "Target attack shows danger of remotely accessible HVAC systems," Computerworld, February 7, 2014, accessed at https://www.computerworld.com/article/2487452/cybercrime-hacking/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html

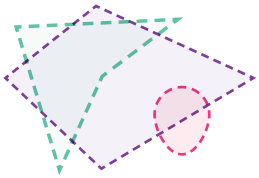
[11] "Researchers Hacked Amazon's Alexa to Spy on Users, Again," Threatpost.com, April 25, 2018, accessed at: https://threatpost.com/researchers-hacked-amazons-alexa-to-spy-on-users-again/131401/.



4. **Existing strategies cannot meet new regulatory requirements.** The regulatory landscape is shifting underfoot. Unnerved by the vast attack on U.S. credit bureau Equifax that exposed the personally identifiable information of approximately 145.5 million Americans and disturbed by the way social media companies have sold access to user data without their users' knowledge or permission, governments are promulgating ever stricter privacy regulations and laws.

   In the EU, the General Data Protection Regulation (GDPR) went into effect on May 25, 2018, requiring organizations with users or customers in the EU to do a better job of protecting customers' personal data. This has forced many U.S. companies to re-write their privacy policies, and in some cases de-identify and encrypt data they already possess.

   In addition, individual countries are passing their own privacy regulations forcing companies to store data on their citizens within those countries' national borders. As a result, corporations that once consolidated as much data as possible within a single controlled location must now operate and secure multiple data warehouses all over the world. This proliferation of data centers both magnifies overhead costs and increases the complexity of blocking hackers from gaining access to steal data or otherwise wreak havoc.

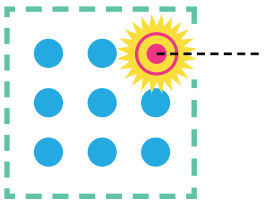


Making Cybersecurity an Integral Part of the Strategy to Transform the Digital Customer Experience

Going forward, a successful cybersecurity strategy will need to have four components:

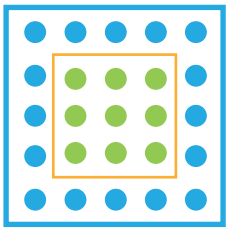
1. Instead of focusing on a warehouse, a facility, a geography or a system, cybersecurity must be **data-centric**. That is, the company must commit to protecting its data and its customers' data wherever it resides.

2. Cybersecurity strategy must become **flexible**. Regulations will continue to change. Connected devices will proliferate. Data will continue to multiply. A company's cybersecurity strategy must be able to change dynamically.



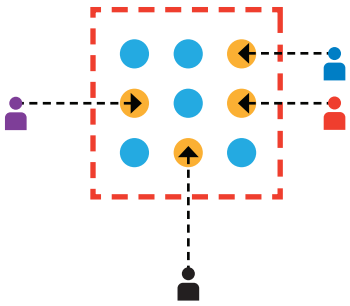
3. Cybersecurity must put a major emphasis on **predictive** capabilities. Ideally, companies should have the cybersecurity capabilities to identify and mitigate risks before they become a problem. What's better than stopping a hacker in his or her tracks? Stopping the hack attack from occurring in the first place.

   Big data and analytics tools have a major role to play in pinpointing problematic transactions and probing intrusions so that companies can take steps to shut down emergent threats.



4. It must be **inclusive**, encompassing the protection of both the company's intellectual property as well as its customer data.

Protecting the organization's data from cyber-attacks starts with an understanding of the internal and external vulnerabilities your business faces. Having a well-rounded strategy and approach, coupled with pro-active threat hunting, will enable organizations to focus their resources on the entry points where hackers can gain entry to systems.



Risk Analysis Baked into the Design

Too few organizations use a risk-based approach when considering which digital systems to implement.

Rather than trying to wrap a security blanket around an inherently vulnerable system, companies should make sure that cybersecurity experts have a key role in designing, building and testing the digital systems and processes used to safeguard IP, protect customer data and keep companies in regulatory compliance.

Gone are the days when companies could relegate cybersecurity strategy to their IT departments; this is a business issue. Organizations need to employ an approach that integrates cyber protection into all aspects of the organization, from employee training to sales to finance to operations.

Complying with Regulations, Weighing the Costs

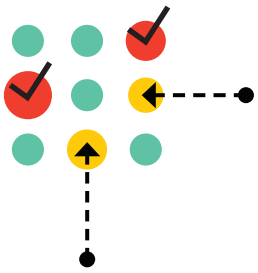
As noted, the EU's new GDPR regulations place new privacy and data protection responsibilities onto corporations.

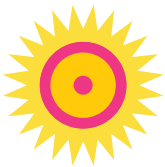
Obviously, companies must comply with all applicable laws and regulations in the jurisdictions where they do business. But as new cybersecurity rules multiply and come into force, companies may need to make some hard decisions about whether it makes financial and strategic sense to do business in certain countries.

For example, some countries are now passing laws saying data on their citizens must reside within their borders. Companies will need to calculate the costs and benefits of complying with those rules:

- What are the financial costs of setting up these new distributed data centers?
- Will the company need to make major changes to its cybersecurity strategy or protocols to move from a few centralized data centers to many far-flung facilities?
- Will the logistical and operational challenges of securing these multiple data centers distract the cybersecurity team from focusing on other, more important threats to its core systems?

In some cases, it could make sense for a company to pull back from non-core markets or countries rather than incur the additional costs, risks and distractions of complying with especially burdensome regulations.





Prioritize, Then Pursue

Every system has flaws. Every program has bugs. The key is to figure out which flaws and bugs are mere annoyances, and which are existential threats.

Whether a company's data lives in a data center or a cloud computing environment, the cybersecurity team must be adept at identifying the most significant risks and prioritizing fixes based on two criteria:

1. Does the risk represent a threat to core business operations? In other words, if a system goes down or is taken offline, will the result be a minor annoyance or a major disaster? Will the repercussions be a minor embarrassment or a major hit to the stock price?

2. Could the threat involve customer data, especially personally identifiable information (PII)? If hackers get access to customers' names, emails, addresses and birth dates, that might not have any discernable effect on day-to-day operations, but it could cause devastating reputational damage and lead to unpleasant regulatory, legal and political repercussions.

By assessing whether threats overlap with either of these two red flag areas—core business operations and/or PII customer data—cybersecurity teams will know where to focus their efforts. Other issues can wait. These are the threats that must be addressed immediately.

Challenges—People, Skills and Frameworks

Cybersecurity teams must overcome two key challenges if they hope to keep their organizations safe from disaster:

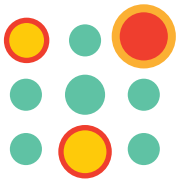
1. **Finding and training the right people.** Currently, companies are having difficulty hiring and training people fast enough to keep up with the pace of change in the cybersecurity world. According to a recent workforce report, there will be a 1.5 million-person shortfall by 2020 in cybersecurity talent.[12]

   Threats are evolving faster and faster. Each new technology comes with a steep learning curve. Yet, at the same time, each new cybersecurity tool has a shorter shelf life than the previous generation. Hardware-based firewalls were the foundation of cybersecurity for a decade but have now given way to software-defined networks where everything is virtual, including the firewall.

   The most important skill that cybersecurity professionals need today is the ability to orchestrate, collect and interpret data from multiple security tools. They need to filter the information and figure out where to take action first, according to the prioritization methods outlined above.

   To address the shortfall of cyber security talent, organizations will have to invest on in-house talent development programs and leverage digital technologies for virtual training. Investments in robust training content and virtual labs on cloud for hands-on trainings are key to a successful talent development program.

[12] "Workforce shortfall due to hiring difficulties despite rising salaries, increased budgets and high job satisfaction rate," (ISC) Study, April 17, 2015, accessed at http://blog.isc2.org/isc2_blog/2015/04/isc-study-workforce-shortfall-due-to-hiring-difficulties-despite-rising-salaries-increased-budgets-a.html



2. **Building a robust rules-based framework.** Security organizations typically find themselves deluged by detected threats. But, as noted, not all risks deserve equal attention. Some can be safely ignored (or at least put on the back burner); others require the undivided, instant attention of first-responders.

   Companies can significantly reduce their cybersecurity risks by making sure they have a strong, rules-based framework in place to help team members properly prioritize security threats and responses. Some sample prioritization rules could include:

   - Prioritize threats to systems that are critical to business operations, including financial and customer transactions.
   - Prioritize threats to systems and databases that contain PII, as breaches in those areas would expose the company to regulatory and reputational damages.
   - Prioritize repairs in systems that connect to the internet, as they are vulnerable to external hackers who can then move horizontally to access a business's entire network or outward to interfere with customer systems.

   Cybersecurity departments will never have infinite resources or infinite time to fix known problems, so having this type of clear, comprehensive rules-based framework plays a critical role in making sure that team members rank risks appropriately and use their time wisely to mitigate the most severe threats.

Enterprises should embed cybersecurity considerations into the design, development and testing of these new customer experiences, and the digital products and services that make them possible.

Start with Security

The overarching challenge facing corporate security leaders today may not be new—customers and users have always wanted maximum access and availability, and bad actors have always probed for ways to defeat defenses—but what *is* new is that the opportunities for mischief and the vectors for crime have multiplied. With data residing everywhere—and increasingly outside the four walls of the business—we live and work in an ever-expanding universe of vulnerabilities, with every point in that universe connected to another. This is both the strength and the weakness of modern technology-driven business.

This increasingly robust and useful web of connected systems and devices presents businesses with a tremendous opportunity to develop new customer experiences to meet expectations and delight consumers. But it also demands that enterprises embed cybersecurity considerations into the design, development and testing of these new experiences, and the digital products and services that make them possible. The best and most cost-effective time to consider the cybersecurity consequences of all these innovative products, services, and experiences is at the beginning, when they are still a gleam in the business's eye, and before something bad happens.

They say that prevention is worth a pound of cure. That's never been truer than it is today.

Authors

Satish Thiagarajan
Vice President, TCS

Sachin Khalap
Head, GRC CoE,
Cyber Security Practice, TCS

Contact

Visit the unit page for more information: https://sites.tcs.com/bts/cyber-security/

Email: BusinessAndTechnologyServices.Marketing@tcs.com

About Tata Consultancy Services (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that partners with many of the world's largest businesses in their transformation journeys. TCS offers a consulting-led, Cognitive powered, integrated portfolio of IT, Business & Technology Services, and engineering. This is delivered through its unique Location Independent Agile delivery model, recognized as a benchmark of excellence in software development.

For more information, visit us at **www.tcs.com**

Experience certainty.

IT Services
Business Solutions
Consulting