How Modernizing Cybersecurity Empowers Business Growth

By Santha Subramoni and Tirath Singh

Essential points

For most companies, cybersecurity has not kept pace with their other transformation efforts. In a digital ecosystem, cybersecurity must leverage the best of what technologies like cloud, artificial intelligence and analytics can deliver in order to fend off the worst that cybercriminals will attempt.

- Many cybersecurity practices are focused on ensuring compliance rather than mitigating risk; they still operate from a basic philosophy of "trust but verify." A more resilient model equal to today's challenges begins from the premise of "never trust, always verify."
- Zero-trust cybersecurity, adaptable to emerging threats and changing access needs, can detect threats in real time and take immediate action to protect an enterprise's data, devices and operations in ways reused passwords and VPNs no longer can.
- The best cybersecurity solutions today are actually services, not just software, and can address an evolving threat profile and support the fast-moving innovation agenda of purpose-driven businesses.

The problem

Traditional corporate cybersecurity has come under scrutiny in today's dynamic economic, social and regulatory landscape. Practices that were established when data, applications, and other elements of IT infrastructure were located within a company's four walls are not sufficient for an era of cloud computing and increasingly decentralized threats. A hyperconnected, boundaryless network is the new normal for a modern digital organization — which means a wider threat surface and more vectors for actors with ill intent globally.

Technology advances — from the Internet of Things (IoT) to artificial intelligence (AI) and advanced analytics — are enabling purpose-driven, resilient and adaptable enterprises. Yet for many companies, IT cybersecurity principles and tools are still an afterthought, continually trying to catch up to the technology disruption. As a result, while business understandably focuses on rapidly pushing new products to market, necessary security standards and governance frequently lag behind.

> Technology advances — from the Internet of Things (IoT) to artificial intelligence (AI) and advanced analytics — are enabling purpose-driven, resilient and adaptable enterprises.

That leaves vital data vulnerable and critical operations at risk. More important, no longer is the threat only to corporate, government and personal information. With the widespread adoption of Internet-of-Things capabilities into our daily lives — including advanced healthcare solutions — even human lives can be at risk.

Cybersecurity during COVID-19 and beyond

The cyberattack risks faced by companies using outmoded security methods have been intensifying in recent years. But those challenges have increased dramatically with the advent of the COVID-19 pandemic.

With so many key employees now working remotely, sensitive data needs to be shared outside a company's walls. This includes employee data, intellectual property, corporate financial data and other proprietary information. It also includes data on customers, their purchases and the performance of products in the field.

Cybercriminals have seized this opportunity by launching phishing schemes that lure email users to click on malicious files. Many of these schemes have been COVID-19 related, and they have ranged from audio files impersonating voicemail targeting Office 365 users[1] to emails purporting to be from company executives. Meanwhile, the number of remote desktop protocol (RDP) servers exposed to the internet has risen sharply from 3 million in January 2020 to more than 4.5 million in May, and attacks targeting them were up more than 300% in the United States in both March and April.[2]

[1] PhishLabs, "COVID-19 Phishing Update: Voicemail Attacks Surface Targeting Office 365 Users," by Jessica Ellis, April 17, 2020, accessed at https://info.phishlabs.com/blog/covid-19-phishing-update-voicemail-attacks-surface-targeting-office-365-users

[2] CSO Online, "Attacks against internet-exposed RDP servers surging during COVID-19 pandemic," by Lucian Constantin, May 8, 2020, accessed at https://www.csoonline.com/article/3542895/attacks-against-internet-exposed-rdp-servers-surging-during-covid-19-pandemic.html

Further complicating the job for security professionals, the ubiquity of bring-your-own-device (BYOD) work protocols allows cyber attackers to leverage outdated and unpatched operating systems or insecure apps on employee machines.[3] For example, a vulnerability recently discovered in the popular iOS Mail app may have been exploited for two years (and possibly nearly eight).[4] Companies also must defend against man-in-the-middle attacks, in which an attacker secretly gets in between a user and an accessed web service. A compromised Wi-Fi system, for example, could let an attacker harvest any information a user sends, including passwords.

Companies also face newer, more sophisticated and pervasive threats. There is a rising incidence of zero-day threats exploiting unpatched software vulnerabilities. Additionally, malware attacks, including keyloggers and ransomware, are leveraging and paralyzing corporate networks. More and more malware seeks to connect IoT devices to botnets that can then create massive distributed denial of service (DDoS) attacks against companies, governments and institutions, resulting in some of the biggest shutdowns across industries ever seen.[5]

The challenge: A vast and growing web of vulnerabilities

In the face of so many threats, companies must secure a vast array of vulnerabilities. Employees themselves can pose risks, whether through poor cybersecurity hygiene or malicious intent. Deeply integrated partners and suppliers, including third-party vendors and their suppliers, can also open the gates to criminal activities. For instance, the breach of 110 million Target customers' personal and credit card data began with malware used to steal login credentials from an HVAC subcontractor. As companies depend on interoperability via the digital ecosystem, the complexity of the threat landscape is deepening.

Criminals can also exploit numerous non-human entities, including (but not limited to) robots, microservices, automated functions, and technologies with system access, such as IoT devices and operational technology. Indeed, there is a multitude of points of weakness in corporate IT systems: outdated and unpatched software; missing or

[3] TechnologyAdvice, "Cybersecurity Trends in 2020: BYOD and Mobile," by Tamara Scott, January 7, 2020, accessed at https://technologyadvice.com/blog/information-technology/cybersecurity-trends-2020-byod-mobile/

[4] CPO Magazine, "Serious iPhone Vulnerability Triggered by Simply Opening Mail App May Have Been Present for Nearly Eight Years," by Scott Ikeda, May 4, 2020, accessed at https://www.cpomagazine.com/cyber-security/serious-iphone-vulnerability-triggered-by-simply-opening-mail-app-may-have-been-present-for-nearly-eight-years/

[5] IEEE Computer Society, "Water Supplies, Smart Grids, Personal Privacy, and Elections As Targets: An IoT Governance Ecosystem Can Improve Security," by Lori Cameron, accessed at https://www.computer.org/publications/tech-news/research/google-amazon-fitbit-security-iot-governance-of-ecosystem

insufficient encryption; insecure SQL databases; data access points (such as web-based applications) and website input fields that allow JavaScript, ActiveX, and other code submissions.

Breaches are intensifying

With so many vulnerabilities to exploit, it's no surprise the number and severity of attacks is on the rise. These have intensified in some of the countries most affected by the pandemic, such as the United States and Italy. Marriott, which has been hurt by the sharp downturn in travel due to the COVID-19 pandemic, was attacked in April 2020, compromising the data of more than 5 million guests,[6] its second major cyberattack in two years. Also in April, Energias de Portugal, one of Europe's largest electricity and gas providers, sustained a cyberattack with thieves demanding $11 million in ransom.[7]

In some cases, criminals are targeting organizations integral to the pandemic response. Hacking attempts at the World Health Organization coronavirus testing lab doubled after the crisis began. A hospital with one of the Czech Republic's largest COVID-19 testing facilities had to shut down after a cyberattack. More recently, REvil ransomware has been used to attack everything from vaccine researchers to unpatched VPN servers. (In 2019, cybercriminals deployed REvil against data centers, managed service providers, local Texas governments and dentist offices.)

The number of security breaches is bound to grow, in part due to the rise of IoT.

The number of security breaches is bound to grow, in part due to the rise of IoT. While IoT hackers primarily exploit router vulnerabilities, they are increasingly targeting hardware that may have never been meant to receive an IP address: webcams, printers, and even electricity meters and gas station pumps. This risk will intensify as 5G makes IoT more pervasive and enables phones to be used as full-scale Wi-Fi networks.

Consequently, as the digital ecosystem continues to evolve, and meeting the growing need for frictionless interactions with customers may lead companies to compromise on security, the philosophy and practice of cybersecurity must change. A blanket lockout of all nonhuman identities and external users puts security inside the castle and

[6] CPO Magazine, "Marriott Hit With Second Major Data Breach in Two Years; Over Five Million Guests Compromised," by Scott Ikeda, April 13, 2020, accessed at https://www.cpomagazine.com/cyber-security/marriott-hit-with-second-major-data-breach-in-two-years-over-five-million-guests-compromised/

[7] SC Media, "Ragnar Locker's well-conceived ransomware attack on Energias de Portugal," by Doug Olenick, April 16, 2020, accessed at https://www.scmagazine.com/home/security-news/ransomware/ragnar-lockers-well-conceived-ransomware-attack-on-energias-de-portugal/

opportunity outside the moat, where opportunities may be lost and cybercriminals may thrive. That sort of comprehensive lockout demands exceptions if business is to continue, and exceptions create vulnerabilities unless they are part of a robust, modern system designed to be adaptable, risk-based and context-aware. And that is where cybersecurity must go.

The solution: Adaptable cybersecurity

Cybersecurity has long been due for a rethink that transforms the concepts of usernames, passwords, and IP addresses, turning them into practical elements that support their underlying functions. The emerging digital ecosystem only became possible as the traditional elements of computing — mainframes, operating systems, applications, and networking — became atomized, abstracted and virtualized. Accordingly, to protect themselves and become more resilient in the face of cybercrime, companies need to consider the broader ecosystem and apply adaptable cybersecurity.

Many security practices are still based on the old concept of trust but verify, yet today data and applications extend far beyond the company's walls and blind trust is a luxury that no business can afford. Instead, cybersecurity should focus on authenticating identities and devices in the context of requests for any protected resource. Such resources broadly include anything that would constitute a risk to the business if it were compromised. This means data, networks and workloads, but also their data flows and the underlying infrastructure that supports them.

Legacy security is not robust enough to secure a contemporary IT ecosystem consisting of remote workers, workplaces, partners and customer interactions, or to protect the data employees may need to access at a remove. In the past, security was based on known employees working from company offices or on a laptop using a VPN. Security functions focused on external threats. Internal errors, threats and leaks were not taken as seriously.

When only company desktops, printers, and on-premises data centers required permissions, that kind of security could manage the challenge. But new vulnerabilities arrive with each advance in technology. Not only are employees using their own devices — smartphones, laptops, tablets and desktops — but companies depend on the operating technology of internet-connected products. Moreover, individual departments are frequently deploying their own robots and other automated entities, outside the umbrella of corporate IT, and their priorities and security diligence may be inconsistent. That's why security must be addressed in the corporate IT architecture.

Under the digital ecosystem, rather than depending on a user's email address and password to grant access to a secure local area network, context should hold the key to access. Context means considering a variety of factors. For instance, what identity needs access, and what is its status? What device is being used? How secure is it? Is it managed? From where is the resource being accessed, both physically and in relation to the network? And when was the access initiated?

Achieving "Zero Trust" cybersecurity

To deploy security that enables an enterprise to focus on its purpose, a Zero Trust Security Model must be applied. Zero Trust protects against unauthorized access to digital resources by enforcing controls that are granular, risk-based and adaptive for each and every access request. Zero Trust relies on six core principles and associated technologies.

1. Never trust. Always verify

Today, nearly all work takes place in a networked environment — which is to say, a potentially compromised environment. Given the profusion, variety and evolution of threats, the secure approach requires validation for any identity before access can be established.

2. Purpose-driven access

Earlier methods, such as a "one-time password" sent to an email address via internet protocols, no longer suffices; they're too prone to compromise. Instead, access must be contextual and time-bound: "just enough" and "just in time" to deliver required business outcomes. Password-less multifactor authentication (MFA) is both more secure and generally faster for users then multiple password resets and insecure email delivery.

3. Continuous risk-discovery, real-time treatment

A "find to fix" approach — automated, with greater agility and operational rigor — should replace the long cycles of audit, testing and remediation most IT organizations have operated under.

The purpose of cybersecurity should be to manage risk to enable business. But most security solutions focus on compliance rather than risk. While compliance is always necessary for regulatory adherence, reporting, and security hygiene, real technology risk is contextual. Only measures that dynamically calibrate controls can address the threats. Access governance must be driven by the risk index of the resource and the risk level of the identity's context.

4. Security by design

As disruption — enabled by new technology and new business models — increasingly becomes the differentiator for growth and capturing market share, the importance of delivering sustainable, secure products and services to end users becomes all the more important, particularly for any innovation touching human lives. Thus, because cybersecurity must be central to the customer experience as well as business continuity, its position has moved to earlier in the development cycle to ensure its priority and enable the delivery of flawless projects.

5. Information-centric security

Rather than focus on their IT, most forward-thinking enterprises aim to focus on their core business, even going so far as to shed assets unrelated to their purpose. Thanks to the proliferation today of cloud-based models for many of their computing needs, businesses can instead center their proprietary information and expertise — their data and its uses — at the core of the business, around which IT services can secure the perimeter.

6. Security as culture

As the saying goes, a chain is only as strong as its weakest link, and a company's data is only as secure as its most vulnerable vector. Beyond making cybersecurity an enforcement issue, a culture of security makes it everyone's responsibility, empowering every user to sense and act on cybersecurity matters.

Implementing adaptable cybersecurity

To this day, most companies' cybersecurity solutions are undifferentiated from most other companies'. While industry standards and state-of-the-art approaches should be the basis for any technical solution, only a business solution can enable the day-to-day work and unique exigencies of a particular company. Based on TCS' work with nearly 500 companies and 7,000 cybersecurity professionals around the world, we have developed an approach to cybersecurity that is both resilient and adaptable.

Insight-led intelligence for human and automated decisions

A deep and comprehensive view of the threats contextualized to a company's business provides the start to ensuring business priorities, followed by identification and measures of risk, complete insight into the highest value assets and processes to prioritize cybersecurity efforts, and a clear strategy for deploying both proactive and reactive capabilities to achieve cybersecurity objectives.

Keeping bad (or reckless) actors at bay

Access to protected assets should require context — the who, what, why, where, when and how definition of a particular request or connection. For example:

- Identity: human, nonhuman, privileged (e.g., sysadmins)?
- Device: laptop, desktop, mobile, IoT sensor — and is it managed or unmanaged?
- Location: on-premises, via internet, from the local plant or from a place the company has no presence?
- Time of day and duration: why is an HR database being accessed for hours beginning at 3 a.m.?

Once access for an asset is thus defined, only then can it be micro-segmented and governed in a Zero Trust context.

Scalable and adaptive access

It may be an understatement to say that, in the face and wake of the COVID-19 pandemic, "work" has undergone some changes. Age-old concepts around workplaces — location dependency, fixed local hours of working, presenteeism and high-touch governance, to name a few — are giving way to a distributed model of the talent ecosystem to maximize business opportunities. [8]

It's a trend that was accelerated by the pandemic, but it was already becoming an increasingly useful model of working for companies emphasizing their expertise over their real estate. Even as some regions and offices began to reopen, working from home was announced as a permanent strategy or employee option for many companies' workforce management policies and practices.

Such a forward-looking approach to work requires an equally forward-focused security strategy, however. This involves establishing scalable and adaptive access independent of device identities and locations. Legacy security solutions such as VPNs cannot adequately accommodate remote workforces. Instead, multi-factor authentication methods and remote-access-as-a-service solutions can address changing security needs as they occur and as the instances for such access increase.

Another essential layer of protection covers agile methods and DevOps by embedding and automating identity, access, threat, and vulnerability management within the development environment. DevOps teams often need to use sandboxes, cloud platforms and untested or open-source software. By securing the containers that hold their work, and by securely managing the "secrets" used to authenticate across the

[8] TCS' own swift transition to remote working in the face of pandemic-related lockdowns was facilitated by its Secure Borderless Workspaces™ operating model. This transformative model enables remote access for employees, sets up a suitable cybersecurity framework and supports all project management practices and systems needed to ensure that work allocation, monitoring and reporting continue as normal.

different containers, tools, platforms and applications involved in development and testing, DevOps teams can navigate their environment more freely while minimizing security risks.

Real-time detection and immediate action

In addition to prevention and protection, companies need to act in real time — the last line of defense. This means plugging vulnerabilities and responding to attacks in an agile fashion. It means leveraging the existing security features of products or adopting quick service-based security options from trusted partners. To address threats in a timely manner equal to the risk — whether it's instantly or over time — companies can find partners that can repair weaknesses and cover compromised points.

In addition to access by humans, companies need to secure the AI, machine learning, automation and analytics they deploy, which are themselves essential to a strategic cybersecurity architecture. AI and machine learning enable real-time detection, instant investigation and immediate response to cyber threats. Secure orchestration and automation provide the advanced capabilities to automate the response to live breaches and advanced persistent threat scenarios.

Resiliency for business continuity

Finally, companies must design and implement continuity, backup, and recovery plans with zero latency for critical infrastructure. This is not only essential to risk management but for compliance as well. Indeed, governments are now issuing mandates for critical IT infrastructure.

Perceived obstacles to risk-focused, context-aware security

There are two main obstacles that are frequently perceived as barriers to risk-focused, context-aware security: budget and the pressures of innovation.

While cybersecurity is generally understood as necessary to business operations, investing in point solutions to address a specific cyber risk is not a sustainable strategy, given the rising variety of threat vectors and vulnerabilities.

Instead, today's cutting-edge cybersecurity is consumption-based. By leveraging cybersecurity-as-a-service, a company can optimize its cash flow while gaining access to the latest defenses, with relevant capabilities usually updated at no additional cost (unlike many commercial off-the-shelf version releases). Moreover, this approach makes it possible to add other services as needed at bundled rates. These as-a-service offerings may include remote access, identity management, vulnerability management, threat intelligence, digital forensics, encryption and multifactor authentication, among others.

Moreover, even though compliance-focused cybersecurity may be regarded as a must-have, it has often been viewed internally as a brake on collaboration, innovation and transformation — a necessary evil for the business. In contrast, the adaptable nature of risk-focused cybersecurity reverses that perception (and, sometimes, reality). Leading-edge cybersecurity practices and services are adaptable enough to meet the demands of fast-moving teams and emerging opportunities. By removing many of the one-size-fits-all constraints of legacy solutions, cybersecurity can instead enable development, collaboration, iteration and modernization in ways that were previously unavailable.

Call to action

Gaining maturity in cybersecurity is a journey. Given the evolving nature of business and forward-looking enterprises (to say nothing of enterprising criminals), the process is perpetual, although the cycle of discovery, definition, development, and delivery gets automated and intelligent over time as a company's security culture and the tools it uses grow and adapt to the changing threats and opportunities.

Discover

A thorough assessment is the first step to helping business leaders understand their readiness for modernizing cybersecurity. Understanding an enterprise's current-state security landscape — its actual threat profiles, business risk and current security landscape — is foundational. Absent such knowledge, a company is left in a purely reactive posture, plugging breaches as they occur.

Define

With a discovery outcome in hand, a directional roadmap can be created to achieve a higher state of security maturity. The roadmap can identify the initial goals that can be implemented in the short term and whether existing tools can be reused to meet the objectives or if new tools are needed. Finally, the roadmap establishes a plan for the tactical and strategic phases of implementation based on the current threat level and the organization's vision of end-state maturity.

Develop

Assuming no urgent threats require extensive and immediate attention, the tactical work to shore up defenses can then be undertaken, often with a scrum team comprising a few allocated resources.

Other areas defined in the roadmap may present less immediate risk to sensitive data but are relatively easy to address so their solutions should be implemented at this stage, rather than when they metastasize into a problem. Many if most lay the groundwork for achieving the more strategic phase of cybersecurity maturity.

Deliver to scale

The work to design and deploy security across an enterprise to support its core purpose and growth — and even its expansion into new markets and sectors, if that's part of its business strategy — must be delivered in a way that can scale both the work and horizontally across functions and operations. To accomplish this, the program to deploy strategic security can expand to multifold streams of scrum teams delivering continuously with accelerated agility to make higher levels of cybersecurity maturity a reality.

There are several initiatives an enterprise might undertake during the strategic phase. One is micro-segmentation, a granular separation of sensitive resources, regardless of their physical location. This can take place at the network, hypervisor or host levels.

A second is Zero Trust Network Access (ZTNA), which entails establishing a software-defined perimeter that helps secure and selectively expose sensitive applications only to authorized and authenticated identities. Context-aware authentication and fine-grained authorization based on risk can be developed at this stage, as well.

A company can also implement just-in-time provisioning to grant access only when and for as long as it is needed, ensuring that privileged identities do not acquire permanent access.

Finally, a company may consider deploying security analytics to extend their security incident and event management capabilities with advanced tools that analyze the behaviors of users and entities such as devices, applications, services, data repositories, and anything else with an IP address.

A secure future

To mitigate risk to their business, most enterprises are continuously investing in new tools and technologies, but most such decisions today are still taken in reaction to peer pressure among the C-suite or to solve a specific problem.

Leading-edge, risk-focused and context-aware security is increasingly available as a service, however, rather than as a one-size-fits-all software solution frozen in time or version number. Forward-looking companies take a never trust, always verify approach to access to their data and processes, acknowledging that threats evolve and require the capabilities available in advanced technology — such as AI, automation, cloud computing, and Agile development — to address them. Through leveraging such services, a business can embrace a more resilient and adaptable cybersecurity model, positioning itself to survive new challenges and take advantage of the opportunities in emerging digital ecosystems.

> Forward-looking companies take a "never trust, always verify" approach to access to their data and processes.

Authors

Santha Subramoni
Global Head, Cyber Security Practices, TCS

Tirath Singh
Global Head, Cognitive Threat Management Services, Cyber Security, TCS

To know more

Visit: **www.tcs.com/perspectives**
Email: **TL.Institute@tcs.com**

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

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

IT Services
Business Solutions
Consulting