Next-generation technologies and cybersecurity

A primer for security program influencers and non-IT executives

By David Grady, Chief Security Evangelist, Verizon Business Group

White paper

Why read this white paper?

New and emerging technologies are driving digital transformation across all industries, moving companies closer to becoming real-time enterprises capable of operating in ways once unimaginable. From artificial intelligence (AI) and 5G to blockchain and machine learning (ML), next-generation technologies are enabling companies to run faster, smarter and better than ever before.

But the learning curve is steep, and even the most seasoned IT professionals can struggle to keep up with what's new and what's next. For non-IT business leaders, all the tech talk can sound like a foreign tongue, even while they are fluent in the language of business.

This white paper aims to demystify a number of new and emerging technologies for people who don't work directly in IT or cybersecurity roles, but who nonetheless influence requirements development and decision-making. More specifically, this white paper explores some of the key cybersecurity implications of new and emerging technologies, with the goal of helping security program influencers and non-IT executives understand the potential risks that come with the rewards of next-generation technologies.

Security practitioners can use this white paper to proactively engage and enlighten their peers in the broader non-IT stakeholder community inside their organizations.

When security program influencers better understand how new technologies can bring both reward and risk, organizations stand a better chance of not allowing digital innovation to outpace security oversight.

From buzzword to business-critical

New and emerging technologies will have a profound effect on businesses and industry in the coming months and years. In many mature organizations, the future is already here. Concepts like artificial intelligence (AI) and blockchain have quickly evolved from vague buzzwords to business-critical applications, and digital transformation is happening at every level of the business in every industry. What follows is a primer about several technologies that non-IT business leaders will be hearing more about in the months ahead, if they are not already.

When security program influencers better understand how new technologies can bring both reward and risk, organizations stand a better chance of not allowing digital innovation to outpace security oversight.

5G

What it is and why it matters

The arrival of 5G wireless communications marks a new era of network connectivity and ushers in what many are calling the Fourth Industrial Revolution. As with previous advancements in wireless communications, the transition from 3G and 4G to 5G will provide dramatic increases in both bandwidth and upload and download speeds, together with extraordinary decreases in latency. 5G is expected to unleash as-yet unimaginable innovation. From autonomous and connected vehicles to remote surgical tools, 5G-fueled applications will fundamentally transform every industry.

Some cybersecurity implications and considerations

While the business possibilities are exciting, the security implications of 5G have concerned some companies. That is why 5G networks are being built with multiple layers of inherent security, from vigorous supply-chain scrutiny to ensure that only secure components are used all the way through to complex authentication and data encryption techniques for devices connecting to 5G. While 5G networks are built to be more secure, 5G-enabled applications and business processes may pose security risks if they are deployed without appropriate security scrutiny and oversight. A poorly secured database or misconfigured application remains a risk even if the connection to it is significantly faster.

The bottom line

Business lines eager to implement 5G-enabled technologies like Internet of Things (IoT) or autonomous network-connected devices (to improve the customer experience or increase operational efficiency) might rush to deploy devices that, unbeknownst to them, have weak security. In particular, outdated firmware (which acts as the brains of many of these devices) can be exploited, leading to network incursions by cybercriminals.

If your security program lacks a robust process to review and approve new technologies or devices before they are connected to the network, your security program may have significant blind spots. Don’t let your company’s “attack surface” grow unchecked in a frenzy to take advantage of 5G. And don’t let innovation outpace security oversight.

Blockchain

What it is and why it matters

A blockchain is a distributed database or public ledger used to record digital transactions, which are linked and secured using cryptography. The transactions are immutable—that is, they cannot be altered retroactively. When information needs to be added or updated, the change is verified, authorized, recorded and sealed off by encryption in a block of data, unable to be edited again. The new block is then cryptographically linked to the previous block to form a chain—a blockchain—that’s a complete, chronological record of all transactions. Perhaps the best-known blockchain is Bitcoin, the digital cryptocurrency. Blockchain technology is ideal for many security applications, including managing digital identities, protecting the configuration of key IT systems and ensuring secure supply chains.

Some cybersecurity implications and considerations

Drawing on some (but not all) of blockchain’s DNA is a new approach to a key element of cybersecurity called machine state integrity, or MSI. Having confidence that the machines that power and protect your business are actually configured the way you think they are is an absolute necessity. Unauthorized and undetected changes to settings in any number of systems can lead to data theft, fraud and unsanctioned wire transfers—and to greater exposure to email-based malware, viruses and phishing campaigns. MSI captures concise “state” information and can continuously monitor machines in an organization’s environment to accurately identify, analyze and flag changes to those systems. Assuring data and system integrity has been traditionally has been seen as a manually intensive and mind-numbing task. Blockchain-inspired solutions like MSI can reduce the burden on staff. When managing digital identities, blockchain can also be used to control access to sensitive systems and data.

The bottom line

Blockchain-inspired security solutions can have a significant positive impact on an organization’s security posture, but the technology itself has a reputation for being complex and abstract. When a security vendor proposes a solution based on blockchain, program influencers should focus on the measurable, practical security benefits and results of the solution. Don't get caught up in the math behind the tool.

5AI – AI and ML

What it is and why it matters

No longer the stuff of science fiction, the terms AI and ML are often used interchangeably. While related, the two are distinct—and they move from buzzword to real business value when applied to cybersecurity challenges.

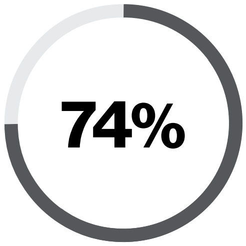
ML is a programming technique that works exceptionally well when an organization has a lot of data to support decision-making, but the humans are struggling to define the criteria to make those decisions. What is commonly called AI is simply the application of ML on a problem—a solution developed using this programming technique. AI and ML are increasingly the driving force behind a number of advanced cybersecurity tools that Chief Information Security Officers (CISOs) and their teams will be advocating to adopt.

Some cybersecurity implications and considerations

AI and ML are behind several new solutions for specific cybersecurity challenges. For example, ML automates many facets of threat hunting, a critical but time-consuming security activity designed to find bad actors who have compromised corporate IT systems. Traditional threat hunting, conducted by humans, often results in a large number of false positives. This “noise” distracts from focusing on the real, hidden threats. ML-driven threat hunting systems may reduce time to detection from 200-plus days on average to just a few hours. And the faster a hacker can be found, the less damage they can do. AI-driven security solutions enable organizations to accelerate and, in many cases, automate their response to cyber incidents.

The bottom line

Like blockchain, the terms AI and ML can seem a bit esoteric to executives and business-line leaders who spend their days focused on non-IT matters. When learning about blockchain-based solutions, program influencers are advised to focus on the tangible benefits of the tools and techniques that leverage AI and ML, rather than the hype or jargon.



of healthcare leaders report that security concerns frequently or occasionally stall digital transformation initiatives.[1]

IoT

What it is and why it matters

While not a new technology, IoT is expected to grow to 25 billion connected devices by year 2025.[2] This will be driven by the global rollout of 5G and by organizations becoming more sophisticated in their use of this technology. Sensors, cameras, intelligent illumination systems and even internet-connected drug-dispensing robots are examples of “things” that can transform the factory floor, the research laboratory, the retail store and the hospital. Many tasks requiring the manual collection of data from far-flung systems can be automated through IoT, thus reducing the costs of moving humans from place to place to collect that data. When data is collected faster, it can be capitalized upon more quickly.

Some cybersecurity implications and considerations

Many security teams struggle to maintain visibility into the multitude of devices already connected to their networks. This struggle is in no small part driven by resource constraints, which include manually intensive first-generation security tools and a global security staffing shortage. With the coming exponential increase in connected devices, security teams run the risk of losing their line of sight into their device population. If deployed with weak security, IoT devices can pose significant security risks. They can be hijacked by botnets and used in denial-of-service attacks (the equivalent of your IoT devices becoming a zombie army). They can serve as a weak-link gateway into core networks. (A well-known example involved a hacker getting into a smart HVAC system maintained by a third party and using it as a lever to steal the details of millions of payment cards from a major retailer.) Espionage-inspired hackers may sabotage the integrity of the data being collected by things, imperiling research—and even causing physical safety risks.

The bottom line

IoT brings a new twist to an old organizational question: Is the security of the technology used to run the business the responsibility of the business line using it, the IT team that manages overall infrastructure or the security team that's concerned with all things security? Organizations must clearly establish who is accountable and responsible for the security of IoT devices, from their predeployment evaluation to their physical deployment, all the way through to the collection, transport and storage of IoT data. The business benefits of IoT are many, so the need is paramount for a solid governance program to oversee how it will be leveraged.

Secure innovation demands collaboration.

Figuring out how to successfully leverage advanced technologies for business gain is the responsibility of all leaders in an enterprise, not just IT leaders. Fostering a learning culture—where people in disparate roles make an effort to better understand the business context and security ramifications of next-gen tech—is an absolute necessity, not a luxury. If businesses embrace new and exciting technologies hastily, they run the risk of innovating themselves directly into a major cyber incident.

You can't embrace the future if your security program is stuck in the past.

New and emerging technologies are at the heart of digital transformation, but in many organizations, digital transformation has outpaced the transformation of traditional cybersecurity capabilities. Many security programs are suffering the effects of a global cyber-talent shortage and are struggling just to do the basics, such as vulnerability management, third-party risk assessments and incident response planning. When a security team can't keep up with the fundamentals:

- It can't find the time to thoroughly evaluate the pros and cons of next-generation tools
- It neglects proactive engagement efforts with stakeholders—and fails to understand the objectives of leaders who are looking to use new technologies to grow their business
- Innovation is derailed as security gets bolted on at the last minute, and not baked in at the beginning when new technology applications are being designed

For example, in a recent Verizon/Healthcare Information and Management Systems Society (HIMSS) survey of healthcare leaders in non-IT, IT and security roles, 74 percent report that cybersecurity concerns frequently or occasionally stall digital transformation initiatives.[1]

Resource-challenged security teams under pressure to support digital transformation efforts are encouraged to consider the benefits of strategic security outsourcing.

Strategic outsourcing is more than just filling empty seats with warm bodies; it's about bringing in experts who can support strategic decision-making and help extract maximum value from legacy (and future) security investments. It's about partnering with a trusted advisor to take a security program to the next level—whether the "next level" means establishing baseline security controls at a small or medium-sized business or transforming a business security program globally.

For more on strategic outsourcing, see our recent white paper, "For Cybersecurity, Strategic Outsourcing Is a Necessity, not a Luxury."

Learn more:

To learn how Verizon partners with enterprises to help protect against today's cyberthreats and prepare for what's next, visit enterprise.verizon.com/products/security/

Or, request a consultation: 877.297.7816

verizon✓

[1] https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf

[2] *2020 Verizon Mobile Security Index*