Critical Convergence

Uniting Cyber- and Physical Security for Optimal Protection

intel.

Authors

Antoinette King, CISSP, PSP

Founder, Credo Cyber Consulting LLC
aking@credocyber.com

Antoinette King has more than two decades of experience in the security industry, holding roles including Engineered Systems Specialist, Operations Manager, Regional Sales Manager, and Key Account Manager. Antoinette founded Credo Cyber Consulting in 2020 with the goal of providing her clients a holistic perspective on security, bridging the gap between the physical and cybersecurity domains focusing on data privacy and protection. Her book, *The Digital Citizen's Guide to Cybersecurity: How to Stay Safe and Empowered Online* reached the Amazon Best Sellers list for all its categories in the first 48 hours of release. She is the recipient of the 2022 SIA Chariman's Award, 2022 ASIS International Karen Marquez Award, 2022 Cyber OSPAs Best Cybersecurity Consultant, and an honoree for the 2022 and 2023 SIA Women in Security Forum Power 100.

Kasia L. Hanson

Global Director, Security Ecosystem Development, Intel Corporation

Kasia Hanson leads Intel's Global Security Ecosystem Development for physical and cybersecurity. She leads the strategy and development of security ecosystem solutions, partnerships, go-to-market and sales acceleration strategies. She is a 24-year veteran of Intel with deep technology expertise across AI, IoT, Information Systems, Cybersecurity, and Datacenter. Kasia is the past-Chair of the Security Industry Association Women in Security Forum Fan Experience in sports, the 2022 SIA Progress Award Honoree, a Women in Security Power 100 honoree, and a Distinguished Fellow for the Innovation Institute for Fan Experience (IIFX) and was named the #3 IFSEC Security Influence in 2021.

Contributors

John Deskurakis
Chief Product Security Officer
John.Deskurakis@carrier.com

Malcolm Harkins
CISO
protect2enable@gmail.com

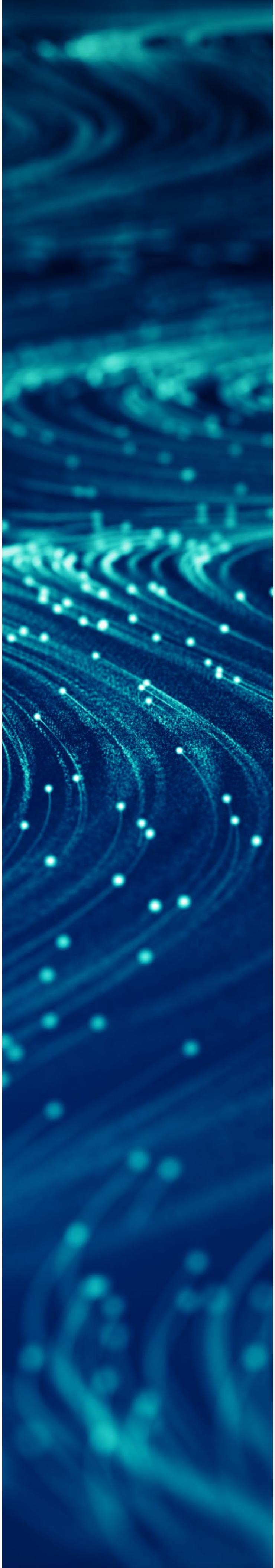
Will Knehr
Senior Manager of Information Security and Data Privacy
will.knehr@us.i-pro.com

Executive sponsor

Rick Echevarria
Vice President, Security Center of Excellence, Intel Corporation

Research consultant

Bridge Partners



Overview
Challenges
Advantages
How to Succeed
Next Steps

Holistic Security

Overview
Challenges
Advantages
How to Succeed
Next Steps

Why follow a unified security posture

Security has never been more important. As threats and risks grow, bad actors are increasingly targeting small to medium organizations through physical and cyber means. For them, the key is finding and taking advantage of any vulnerability. The tiniest opening can lead to a major incident.

The cost of remediating security incidents is on the rise. Spending on cybersecurity is expected to reach $458.9B by 2025[1] with costs including regulatory fines for loss of sensitive data, business downtime, and reputational damage. If security protections aren't part of the foundational principles of your organization's strategy, your whole organization could be exposed.

Security threats are continuously evolving, both in number and complexity. New attacks emerge and existing threats are modified to work in new ways. Every product, every connection, every associate offers the potential for security risks and vulnerabilities. Maybe it's a warehouse door that was propped open when it should have been fully closed, or an employee who unknowingly provides sensitive data to a hacker. At the same time, attackers are targeting potentially softer, lower stack resources, and attempting to exploit physical vulnerabilities. We've seen a steady progression from software and applications to operating systems and middleware, down to the BIOS and firmware level and now the hardware itself. Today's most challenging threats can be a result of hybrid attacks that target both physical and digital attack surfaces.

The broad adoption of the Internet of Things (IoT) and the Industrial Internet of Things (IIoT) has created an interconnected ecosystem of physical and cyber systems, blurring the boundaries and intertwining physical security and cybersecurity. It's predicted that there will be new ransomware attacks every two seconds by 2031.[2] These attacks can not only cause catastrophic loss of data but can also bring an organization's operations to a standstill.

This interconnected ecosystem impacts operational technology (OT) systems, such as physical access control and video surveillance systems, and as a byproduct, physical security operators and teams.

As physical security and cybersecurity are increasingly interrelated, it's no longer viable to separate cybersecurity and physical security policies and practices. A gap between them is dangerous. While the cybersecurity team may be responsible for managing and securing intelligent devices and data sets, the physical security team may not be aware of the need to apply the organization's cybersecurity best practices to their IoT and IIoT devices. Physical security traditionally been more focused on the functionality of technology rather than the security of enabling those devices because they were primarily analog. For example, security cameras once recorded images on videotape which was highly secure because of not being connected to a network. Now cameras are intelligent devices connected to networks as part of a complex ecosystem of technology. Safeguarding such a camera should be a responsibility jointly shared by the physical security/ facilities personnel and cybersecurity team.

Today's reality is that you cannot have a sustainable, effective security posture that includes only cyber- or physical security. Surveillance, defense, risk assessment, vulnerability assessment, business continuity, and access control are critical concerns for both physical and cybersecurity. These domains are two sides of the same coin. The future of the security industry is dependent on the convergence of these two presently separate domains. With threats to an organization's digital and physical assets, holistic security is needed to prepare for modern security risks. A joint strategy should simultaneously limit access to physical assets and property, while also implementing digital safeguards the sensitive data contained within physical systems.

Overview
Challenges
Advantages
How to Succeed
Next Steps

The Internet of Things

Today's computing powers are growing at the edge

40.2%
Business and manufacturing
Real-time analytics of supply chains and equipment, robotic machinery

30.3%
Retail
Inventory tracking, smartphone purchasing, anonymous analytics of consumer choices

8.3%
Healthcare
Portable health monitoring, electronic recordkeeping, pharmaceutical safeguards

7.7%
Security
Biometric and facial recognition locks, remote sensors

4.1%
Transportation
Self-parking cars, GPS locators, performance tracking

Source: Information Systems Engineering, Inc.

Security is a business imperative

Security matters: to customers, to their customers, to governments—and to your competitors.
Customers are demanding security. Security threats and vulnerabilities make headlines with numerous companies receiving publicity for high-profile breaches. Organizations of all sizes are dealing with growing threats. And increasingly, customers want to know how the companies and vendors they choose will protect their systems and data.

An unprecedented amount of legislation, executive actions, and requirements are in development in federal and local governments, focusing on network security, incident reporting, hardware, product assurance, and supply chain/software security. Governments are seeking to increase control in light of serious security incidents (e.g. ransomware) and the increased reliance on digital infrastructure, including for national security.

With heightened customer demand and government regulation, competitors across industries are recognizing that security is a requirement, not just a value-add. Those who can demonstrate their ability to earn and maintain customer trust will drive competitive advantage.

Challenges of the Siloed Security Approach

A siloed security approach means that the physical and cybersecurity departments operate independently. Traditionally, this happens when the physical security professionals see the cybersecurity/IT department as roadblocks to progress. A common physical security approach has been the creation of independent and segmented networks for physical security technologies, while excluding the cybersecurity/IT department from the network design and implementation. This is what is referred to as shadow IT, IT infrastructure created without the knowledge of the IT and cybersecurity departments.

As time goes on, these shadow IT networks increase the attack surface of the organization because they are typically not secured in a manner that adheres to the best practices of the organization. Attack vectors evolve and even if someone stood up the shadow network perfectly on day one, it will progressively become easier to attack over time. This is especially acute because the shadow network runs without the expert support and vigilance of a dedicated cyber team and IT professionals who will evolve controls and protections to meet the ever- changing needs of a complex and dynamic threat landscape. This fragmented approach also creates friction and animosity between the two organizations as the cybersecurity team is ultimately responsible for the security of the organization's infrastructure. Shadow IT increases risk and likely makes the organization vulnerable to attack. Some of the drawbacks to operating independently include:

Siloed roles/role clarity

Your physical and cyber assets pose a significant amount of risk to the organization. Each can be targeted, separately or together, to compromise your systems and infrastructure. Since so many organizations treat the two sides of security as separate challenges, security leaders often operate in siloes without a holistic view of the threats targeting their organization. This can leave enterprises more vulnerable to attacks that can lead to the exposure of sensitive information and intellectual property, disruption of business, and/or reputational damage.

Siloed communications

Without a full understanding of the greater threat landscape of the organization, disparate security departments may be unwittingly operating against the best interests of the organization. Inconsistent communication and limited information sharing between two separate security teams may lead to increased vulnerability and risk to the organization. Strong coordination between the cyber- and physical security teams can dramatically improve the overall security posture of the organization.

Remote workforce risks

Mobile workers, some of whom are using their own devices, may or may not follow cybersecurity or physical device policies. These policies can be difficult to enforce among multiple locations and employees without the proper controls in place. Adding in the potential for human error, remote workplaces can be an extension of the attack surface.

Economies of scale

Staffing, equipping, training, and maintaining two separate security teams can be expensive. Additionally, there may be duplicated efforts which can result in increased costs and inefficiencies. Missed opportunities to protect your organization are even costlier.

Incident response delays

Security incidents often intersect both physical and digital domains. Responding to incidents and incursions can be ineffective and slow without a unified team. A lack of collaboration between the cyber- and physical security teams will result in delays in communication and response efforts.

Advantages of the Holistic Approach

Physical security and cybersecurity go hand in hand. With formal collaboration between the previously separate security functions, organizations can be more efficient and resilient. They can better anticipate, identify, mitigate, and respond to threats. Unifying security policies across divisions bolsters more success in fending off exploits. Most importantly, your security capabilities will be more robust. Convergence is the best defense.

You get a greater return on your security investment. Eliminating redundancies and getting a more thorough understanding of vulnerabilities can result in considerable savings. A combined cyber- and physical security team gives you more efficiency by reducing task duplication and freeing up the team to focus on its most important tasks.

Security generates opportunity. While conventional thinking says security is defensive, increasingly it's being used as a proactive approach to unlock business opportunity. When your systems and data are safeguarded, it frees you to do what you do best and unlocks new ways of working.

For example:

- Reduce risk and accelerate your business. When you address security threats, protect IP, and reduce the risk of exposing sensitive customer and employee data, you can improve efficiencies when data is generated and shared.
- Collaborate in new ways with new partners. Selecting solutions that help you protect data in transit and in use makes collaborating with your partners more secure.
- Innovate new products for your customers. Security means more than better ways of doing things. It means entirely new ways of working, including previously unavailable products, services, and solutions.
- Be a stronger partner in your customer's ecosystem. By committing to robust security practices, you become a stronger partner to your customers. Increasingly end users are focused on securing their supply chain. By focusing on holistic security throughout your organization you make your organization more marketable.

Having a strong security posture is essential and protects against ever-increasing threats to your interconnected infrastructure. A comprehensive approach to security enables a flexible, sustainable, and successful security strategy.

Benefits for enterprises include:

- Reduction in duplicative efforts and increase in productivity
- Meeting critical governance, compliance and regulations (GRU)
- A continuous view of the security posture of your organization
- Strategic alignment of risk and threat management
- Safe transition to the cloud
- Defense against 3rd-party breaches
- Cost savings
- IP protection
- Increased trust
- Business continuity
- Data privacy

Overview
Challenges
Advantages
How to Succeed
Next Steps

How to Succeed

Security has generally been considered both a cost center and a roadblock to progress. This does not have to be the case.

Adopting a resilient, holistic security program that incorporates physical and cybersecurity principles should be seen as the guide rails by which your organization operates. This guiding program will provide many benefits for your organization including:

- Alignment with business objectives
  Ensure that the security program aligns with the business objectives of the organization. By doing this, it is easier to get executive sponsorship and top-down support.
- Services growth
  By streamlining security as part of day-to-day business operations, your organization will be able to grow services and be more innovative for your customers.
- Business enablement
  Build trust in your brand by making strong security part of the cultural fabric of your organization. Using security as an essential benchmark for your business can support business growth and innovation.
- Results-oriented cooperation
  Creating harmony between the physical and cybersecurity departments will support results-oriented cooperation. This will make your security posture stronger and more effective.
- Efficient incident response
  By ensuring that everyone is playing on the same team, in the event of an incident, response will be more efficient. Teams will be working together, roles will be clear, and responsibilities will be understood.

Intel: a longstanding commitment to security

As external threats grow in complexity and precision, the growth of AI and Edge/IoT (Internet of Things) devices is adding additional risk by expanding the potential attack surface. Building a strong community of partners is critical—whom you work with matters. Every component, from silicon to software, will play a role in securing data and maintaining device integrity—security solutions start at the foundation (hardware) and build up the stack. Now more than ever, physical and cybersecurity must work together to deliver complete infrastructure and data protection capabilities.

As the ecosystem and solutions evolve and advance, driving a holistic security approach that creates empowerment, enablement, and partnership will help accelerate solutions to security's biggest challenges. Intel's security vision encompasses a holistic undertaking to establish a first-of-its-kind security capabilities and framework, supported across product types and families. This vision is anchored by four pillars:

- **Integrity and trustworthiness**, including efforts for establishing a verifiable foundation of trust in a system.
- **Any data, anywhere—workload protection** with emphasis on securing data, as it is used in new and novel ways.
- **Disruption-free security** to tackle usability impediments to security.
- **Solutions—security your way**, focused on innovation and flexibility to empower choice in customers and developers.

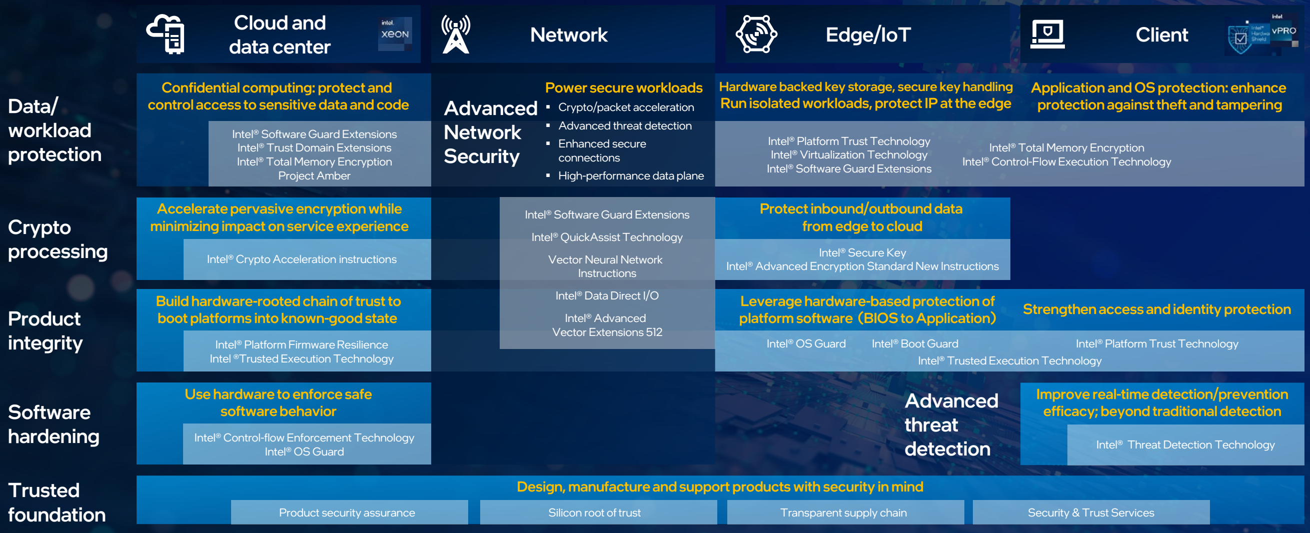
This vision helps ensure Intel's ability to deliver best-in-class security far into the future. This security technology vision goes beyond silicon, reflecting Intel's leadership across the cloud to intelligent edge to client and all through the stack. **Security begins with Intel.**

Overview
Challenges
Advantages
How to Succeed
Next Steps

A longstanding commitment to security

The most comprehensive silicon-based security portfolio

Intel® technology creates a secure foundation with layers of defense spanning cloud to edge



Cloud and data center | Network | Edge/IoT | Client

Data/ workload protection

Confidential computing: protect and control access to sensitive data and code
Intel® Software Guard Extensions
Intel® Trust Domain Extensions
Intel® Total Memory Encryption
Project Amber

Advanced Network Security
Power secure workloads
- Crypto/packet acceleration
- Advanced threat detection
- Enhanced secure connections
- High-performance data plane

Hardware backed key storage, secure key handling
Run isolated workloads, protect IP at the edge
Intel® Platform Trust Technology
Intel® Virtualization Technology
Intel® Software Guard Extensions

Application and OS protection: enhance protection against theft and tampering
Intel® Total Memory Encryption
Intel® Control-Flow Execution Technology

Crypto processing

Accelerate pervasive encryption while minimizing impact on service experience
Intel® Crypto Acceleration instructions

Intel® Software Guard Extensions
Intel® QuickAssist Technology
Vector Neural Network Instructions
Intel® Data Direct I/O
Intel® Advanced Vector Extensions 512

Protect inbound/outbound data from edge to cloud
Intel® Secure Key
Intel® Advanced Encryption Standard New Instructions

Product integrity

Build hardware-rooted chain of trust to boot platforms into known-good state
Intel® Platform Firmware Resilience
Intel ®Trusted Execution Technology

Leverage hardware-based protection of platform software (BIOS to Application)
Intel® OS Guard
Intel® Boot Guard

Strengthen access and identity protection
Intel® Platform Trust Technology

Intel® Trusted Execution Technology

Software hardening

Use hardware to enforce safe software behavior
Intel® Control-flow Enforcement Technology
Intel® OS Guard

Advanced threat detection
Improve real-time detection/prevention efficacy; beyond traditional detection
Intel® Threat Detection Technology

Trusted foundation

Design, manufacture and support products with security in mind
Product security assurance | Silicon root of trust | Transparent supply chain | Security & Trust Services

Intel's commitment to security has never been stronger. We invest in unparalleled people, processes, and products, integrating security in the way we work and everything we work on. As we relentlessly pursue the best solutions to protect customer systems and data, you can be confident Intel is committed to:

Unwavering customer focus

We put customer needs first in our security decisions. We listen to their challenges and use this feedback to guide everything we research, architect, build, and release. Trust is rooted in transparency. We communicate security advisories and product updates to help customers stay informed and keep their systems protected.

Continuous technology Innovation

New threats will emerge and vulnerabilities will be found, so Intel is committed to growing, adapting, and relentlessly advancing security. From accelerating cryptography and Confidential Computing, to safeguarding our supply chain and manufacturing operations, we never stop innovating.

Security by design

We follow rigorous policies and procedures spelled out in our Security Development Lifecycle (SDL) to integrate security principles and privacy tenets at every step of hardware and software development. Intel has dedicated experts driving a security-first mindset that starts with research and design and doesn't stop until products reach end of servicing.

Robust incident response

We invest extensively in vulnerability management and offensive security research for the continuous improvement of our products. Our Bug Bounty program is one critical way we get outside perspectives, collaborating with researchers and leading academic institutions to find and address vulnerabilities. Intel role models best practices for incident response; when an issue is identified, we follow coordinated vulnerability disclosure practices to release findings and mitigations together.

Community advocacy

It's clear no single entity can solve complex security challenges alone. We work with technology partners, academic institutions, industry organizations, and governance bodies worldwide. These efforts support development of policies, industry guidelines, standards, and research to elevate shared security goals that benefit everyone.

We actively work to deliver security without sacrificing performance. Collaborating with our customers and industry partners, we can achieve levels of secure performance people expect and deliver technology they trust.

Closing

The convergence of cyber- and physical security is the future of security. Connecting these two formerly separate functions enables enterprises to address shared critical concerns—surveillance, defense, risk assessment, vulnerability assessment, business continuity, access control.

With frequent, new threats to organizational assets arriving both digitally and physically, a joint security strategy helps safeguard organizations from modern threats. What was secure yesterday may not be safe today or tomorrow. Security is not a one-size fits all operation. It is a constantly changing landscape of threats and risks. As such, solutions will not be the same for every organization. Intel's vision is to provide a customizable, configurable, and updateable security solution that can be tailored to the evolving needs of each customer, based on their specific deployment scenario and threat model.

Convergence between previously separate security functions empowers enterprises to be more resilient and efficient. A unified team and infrastructure can better anticipate, mitigate, and respond to threats, both digital and physical.

Considerations for system integrators

Over 95% of all cybersecurity incidents happen because employees allow threat actors to gain access to their networks through social engineering or manipulation. In my opinion, the most impactful cybersecurity defense to deploy for organizations (particularly small companies) is cybersecurity education, awareness, and training for their employees.

The objective is to convert the organizations employees and leaders into cybersecurity threat hunters, to always be aware of who the threat actors are, and the types of attack the bad actors use. This defense mechanism is non-technical, inexpensive, and easy to deploy.

For system integrators, the conversation and training for installation and service teams goes much deeper on protecting and hardening system deployments and IoT devices on customer networks.

Once you establish cybersecurity awareness and education, I strongly recommend deploying a comprehensive Managed Detection and Response (MDR) service. In a nutshell, MDR leverages AI to monitor the users' network Embedded Configurable Operating Systems (ecos) for indications of attack and quickly mitigates and contains the threat.

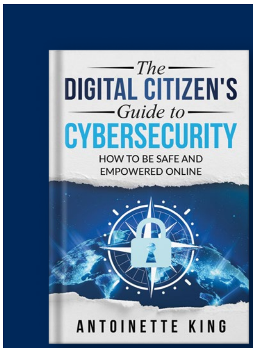
Gary Hoffner
Vice President, PSLA Security

Defining and executing a holistic security strategy offers significant benefits, including better defense against breaches, improving incident response efficiency, meeting essential compliance requirements, and more. Intel believes that a successful security transformation requires certain key components: the right level of stakeholder participation, clearly delineated priorities and policies, and methodical integration of security teams and technology infrastructure.

Intel's vision is to not only empower organizations through our portfolio of security technologies, but also to lead the industry in solutions that solve our customers' most critical business security needs within our partner ecosystem. Intel solutions bring together the power of Intel components, leveraging the hardware's advanced capabilities, data, and telemetry, to deliver solutions that software alone cannot provide.

This document introduced Intel's approach for safeguarding organizations with converged cyber- and physical security. Intel is committed to the relentless pursuit of the best solutions to protect customer systems and data. A successful optimization strategy will bring together people and technology to integrate holistic security in the way enterprises work and everything they work on.

Learn more about Intel security: intel.com/security



The Digital Citizen's Guide to Cybersecurity

At this moment, you are connected to more humans than ever before in recorded history. The phone in your pocket, the laptop on your desk, and even the watch on your wrist connect you to a global community you can contribute to anytime you have a thought worth sharing. As thrilling as this is, the online world can also expose us to a torrent of scary happenings, such as identity theft, misinformation, and intrusive data collection.

Fortunately, the vast majority of online dangers can be prevented with basic knowledge and critical thinking skills. The ultimate manual for practicing safe cyber hygiene, The Digital Citizen's Guide to Cybersecurity serves as an actionable guide to all things Internet for all ages—walking you through information sharing, your digital footprint, and how to recognize and protect yourself from the most prominent online scams. No matter whether you're a tech whiz or someone who struggles to keep up with all of the new gadgets, you too can reclaim control over howyou engage online.

Then, together, we can create a safer, more positive digital world.

Endnotes

[1] https://cybersecurityventures.com/cybersecurity-spending-2021-2025

[2] https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics

Overview
Challenges
Advantages
How to Succeed
Next Steps

THINK EXPONENTIALLY

...not just smarter, but **better** security

BE BRAVE

Get going with projects and opportunities

ACT WITH PURPOSE

Learn, adjust, **iterate**

Notices & Disclaimers

Intel is committed to respecting human rights and avoiding complicity in human rights abuses. See Intel's Global Human Rights Principles. Intel's products and software are intended only to be used in applications that do not cause or contribute to a violation of an internationally recognized human right.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.