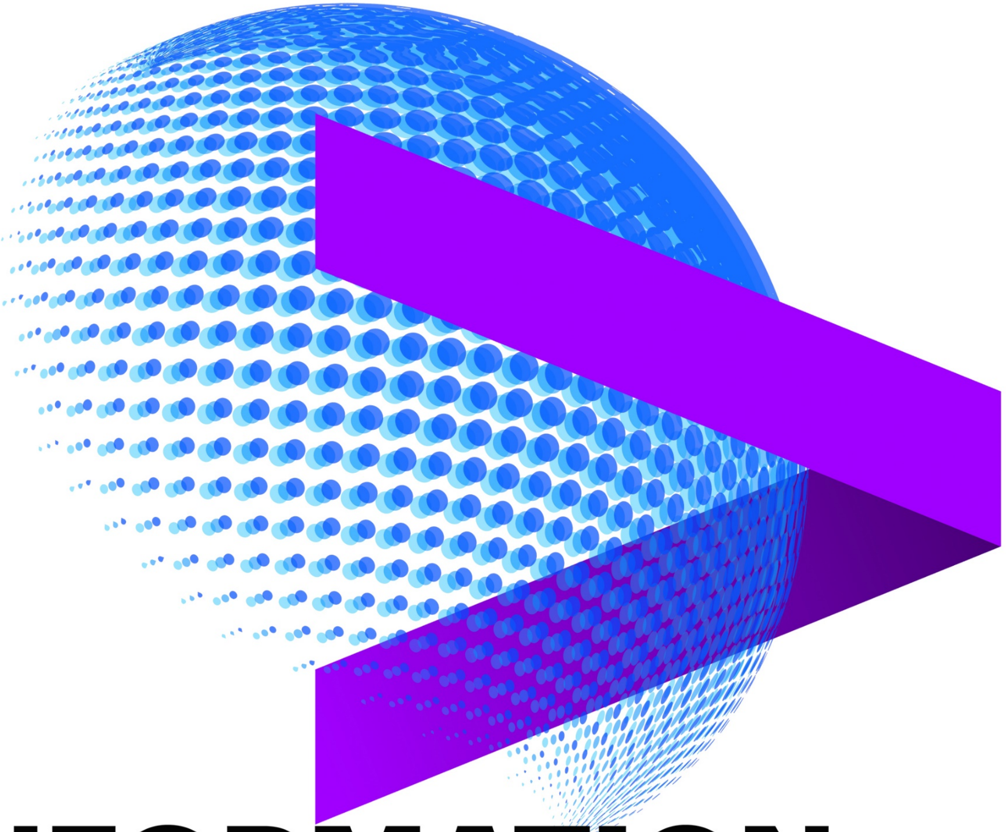
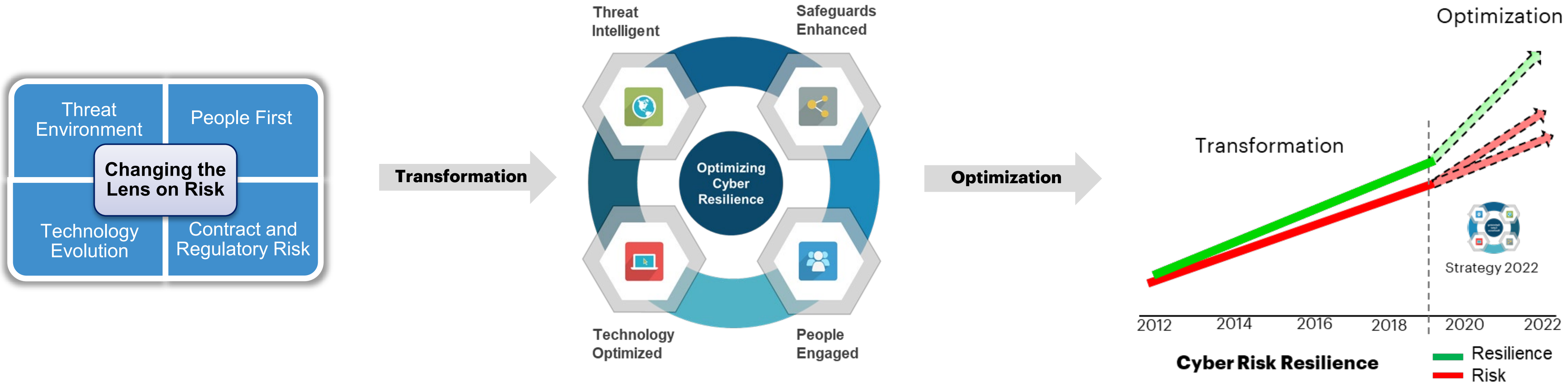
INFORMATION SECURITY STRATEGY 2022

MARCH 2019



INFORMATION
SECURITY

STRATEGY 2022: OPTIMIZING CYBER RESILIENCE



FROM		TO
Strategic benchmarking against high-performing companies	New Strategy	**Defining** and exemplifying **best-in-class risk resilience**
Meeting contractual obligations and adhering to internal standards		**Elevating** the risk evaluation and safeguards required for client service business and the enterprise
Incremental mitigation of identified risks		**Rapid** risk reduction aligned to top threats and prioritized risks
A highly effective risk **detection and remediation** operation		A **Secure from Start** focus on **preventing incidents and vulnerabilities**
Centralized risk identification solutions and processes		Threat intelligent **distributed** security solutions
Early adopters of threat hunting techniques		**Integrated** vulnerability and malicious activity **hunting and discovery**

STRATEGY 2022: OPTIMIZING CYBER RESILIENCE

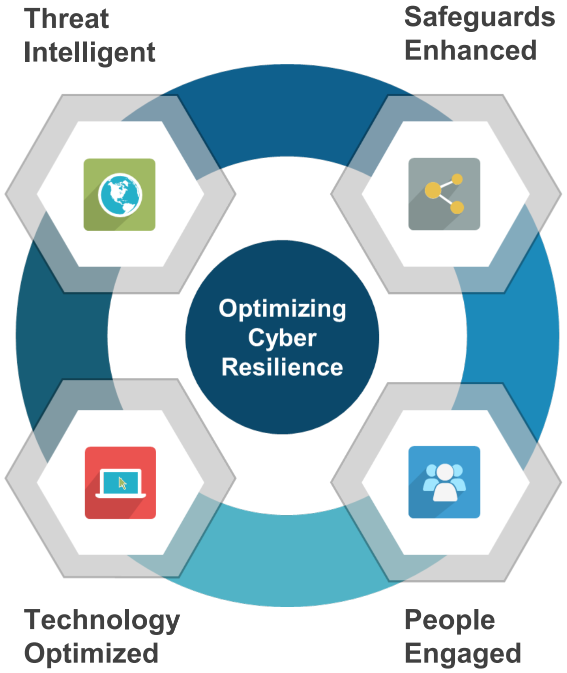
Establishing a best-in-class level of cyber risk resilience through Secure from Start, rapid risk reduction, and pervasive security

A Cyber Security role model

Accenture is a demonstrably mature, cyber risk resilient entity. Our ability to achieve enterprise-wide risk mitigating goals against **rapid business growth** sets us apart from most other entities. Meeting Strategy 2020 objectives allowed us to achieve a **role-model level security posture** and to redefine our approach for maintaining and improving our cyber risks resilience. We are now positioned to begin managing risk with a goal of **Secure from Start**. We will seek to stop preventable risk from being introduced into the environment. We will **proactively identify risk** using hunting and integrated solutions. Risk mitigation will be **rapid**, commensurate to the level of risk.

Cyber Risk Resilience

- ✓ **Threat Intelligent** – A threat intelligent organization adapting to changing threats, making risk-based strategic and tactical decisions
- ✓ **Safeguards Enhanced** – Drive an evolution of security governance through enhanced due diligence and safeguards across client service business and the enterprise
- ✓ **People Engaged** – Moving beyond awareness with people actively engaged to effectively mitigate cyber-related risks
- ✓ **Technology Optimized** – The right technology in the right place at the right time to prevent or discover vulnerability, to realize zero tolerance goals



Establish an industry leading definition of cyber risk resilience

- ✓ Develop a new composite security posture/resilience measure accounting for Accenture's rapid growth and change
- ✓ Use new measurement to direct change internally and influence change externally (establishing role-model status)

STRATEGY 2022: OPTIMIZING CYBER RESILIENCE

PRINCIPLE DRIVERS

SECURE FROM START

Zero tolerance goal for preventable incidents and vulnerabilities

Enhanced metrics, reporting, and tools to drive prevention from the start

Drive business dimension accountability via near real-time data

Individual decision-making based on preventive operational expectation embedded in organizational DNA

RAPID RISK REDUCTION

Zero tolerance goal for identified higher risk vulnerabilities

Commitment to agile remediation

Achieve quicker step changes in driving down risk at digital speed

Enable accountable owners with the tools and process needed to achieve agility in securing Accenture

PERVASIVE SECURITY

Zero tolerance goal for security gaps – the right security, in the right place, at the right time

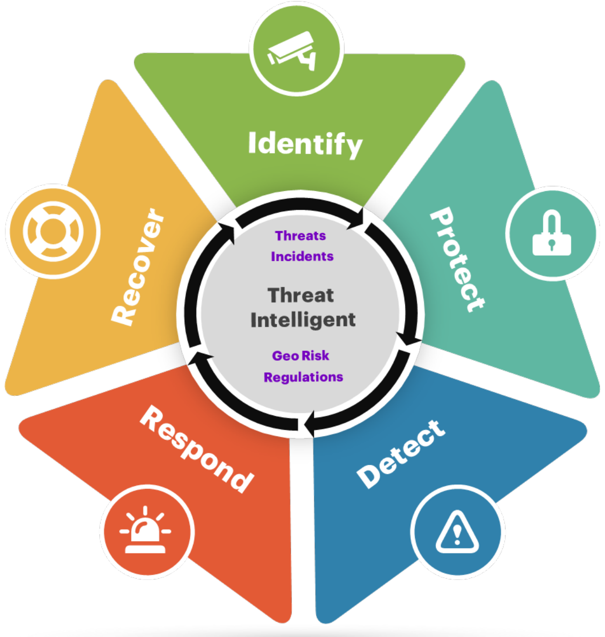
Achieve consistent security hygiene across people, process, and technology even as we strengthen our best in class security function

Drive risk reduction through threat hunting across multiple dimensions of the organization

Evaluate and maintain our core infrastructure, controls, and processes as we evolve

STRATEGY 2022: THREAT INTELLIGENT

A threat intelligent organization adapting to changing threats, making risk-based strategic and tactical decisions



The threat landscape expands to include exponential increases in geographical risks and regulatory requirements

- **Employ a data-driven approach** integrating strategic and tactical cyber threat intelligence and client incident impact analysis to inform risk-based decisions and automate defenses
- Analyze and adapt to **geographical risks**, including: geopolitical climate, state-sponsored threat actors, and geo-specific infrastructure/data security
- Analyze and proactively address the impact of **privacy and cybersecurity regulations** to Accenture and client operations

Threat intelligence informs risk-based strategic and tactical analysis and decisions

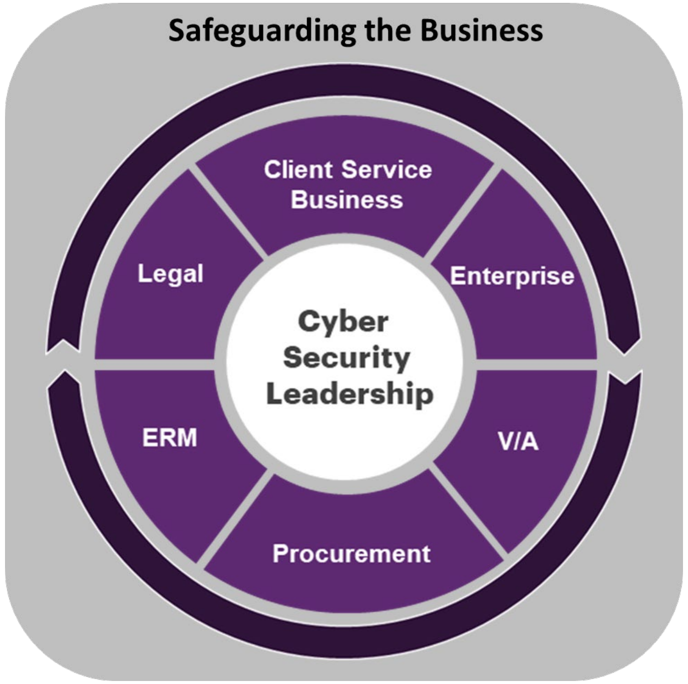
- Develop **strategic viewpoints** that address specific cyber-related concerns which require detailed analysis and consideration, such as: regulatory impacts, evolving threats, disruptive technologies and industry trends
- **Inform** new client and acquisition due diligence, further enhancing risk-based decision making
- Conduct threat intelligent, scenario-based risk assessments against core infrastructure, assets and existing controls to promote effective and **pervasive security**
- Analyze and update cyber security policy and standards to defend against current threats
- **Evaluate and reduce complexity** in security processes to better enable execution

STRATEGY 2022: SAFEGUARDS ENHANCED

Drive an evolution of security governance through enhanced due diligence and safeguards across client service business and the enterprise

Drive ubiquitous security and risk reduction at hacker speed

- Enhance cyber due diligence for client service business and enterprise activity to inform risk based business decisions (go/no-go)
  - Develop sales cyber due diligence requirements for AO/IO/BPO and emerging services
  - E.g. Risk Assessments, automated scanning, contract reviews
- Drive a reduction of contract and controls complexity in client engagements
- Develop risk management oversight processes designed to ensure that threats/risks are communicated to and acted upon (at hacker speed) in accord to zero tolerance goals
- Collaborate across functions to mitigate broad cyber related risks and drive threat intelligent decisions
  - E.g. Client Service Business, V/A, Physical Security, ERM, Procurement, Legal
- Develop and report new composite security posture/resilience scores that inform and action each operating group and business entity



Safeguarding the Business

Enhance the external security ecosystem between Accenture, Clients, Suppliers, Alliance Partners, and government institutions

- Develop enhanced CISO to CISO forums with top clients, suppliers to better share relevant industry learnings and threat data
- Partner with key clients to conduct mutually beneficial risk assessments and controls comparisons
- Develop opportunities where experience in Threat Intelligence, Cyber Incident Response Readiness, and best practice implementation can be shared, exercised, and improved

STRATEGY 2022: PEOPLE ENGAGED

Moving beyond awareness with people actively engaged to effectively mitigate cyber-related risks

Drive Agile Risk Reduction and Secure from Start into DNA of our people

- Enable accountable parties to self-assess security compliance and deliver **Secure-from-Start** solutions
- Validate that global polices, standards, and process are continually being followed and maintained at every level and corner of Accenture
  - Evaluate the benefit of aligning client account security leads to Global Information Security in order to embed security even further and enforce global security posture and hygiene
- Build resilience by minimizing the impact of high severity incidents
  - Target a reduction in high volume low severity incidents and events

Continue to strengthen our People who are the first line of defense against cyber risk

- **Drive down bad security hygiene** by utilizing enhanced metrics and real-time data streams, **including enhanced behavioral analytics**, specific to our Operating Groups and Businesses (e.g. password sharing, phishing, cloud configurations)
- Incentivize individual actions and decisions through a reward/penalty system
  - Evaluate the opportunity for direct rewards, such as monetary awards, recognitions, and consequences (e.g., performance penalties that drive optimal security behavior)
- Continue to provide our people engaging and pertinent security training and awareness
  - Develop and require role-based training to more precisely improve individual security behavior

STRATEGY 2022: TECHNOLOGY OPTIMIZED

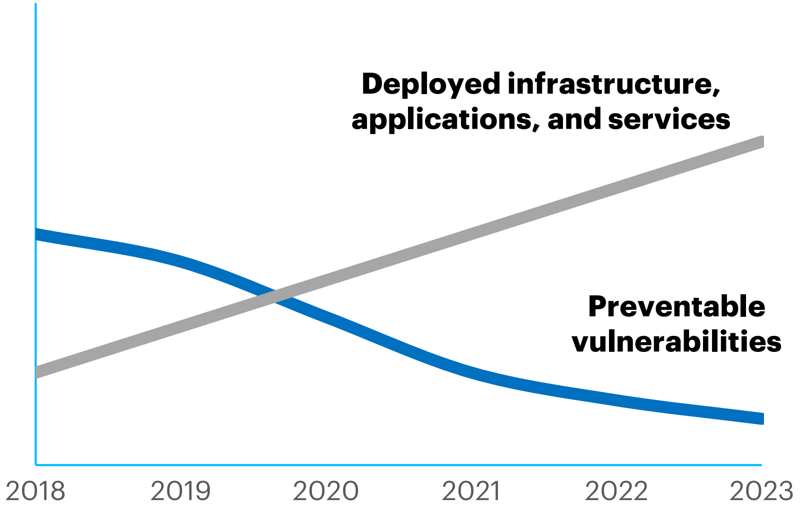
The right technology in the right place at the right time to prevent or discover vulnerability, to realize zero tolerance goals

Optimize our technology stack to drive prevention first expectations

- Achieve **Secure from Start** by driving down common out-of-the-gate vulnerabilities from new infrastructure and services being deployed
    - **Prioritize prevention** of workstation, application, internet, and cloud vulnerabilities at the outset
- Evaluate areas where efficiency might be gained through common platform usage and tool consolidation

Integrate threat intelligence and digital technologies to automate defense

- **Automate** identification, response and remediation capabilities to counter evolving threats and human performance limitations
    - Evolve to intelligent automation and orchestration technologies (Artificial Intelligence, machine learning, and predictive analytics)
    - Identify and respond in seconds (not hours or minutes)
- Prioritize intelligent analytics to rapidly detect and analyse advanced threats
    - Enhance intelligent **analytics** solutions by integrating threat intelligence to identify threats and inform risk decisions
    - Enable threat intelligent risk-based hunting, discovery, and remediation



Secure from Start