Cyber-Security Summit

Building a Strong Cyber Culture

Accenture

Speaker & Topic

Didier Rutagarama, CISA, CISM
Manager

Didier.N.Rutagarama@accenture.com
Accenture Security

Information technology and cyber-security executive with over 11 years of experience and expertise in business, technology, cyber-security operations, and transformation. Didier is passionate about collaborating with public and private sector organizations to rapidly increase the resiliency and reliability of cyber-defense and recovery capabilities. Additionally, he is passionate about developing and embedding security into every business and technology function from the cloud, application development, migration, and operations. His expertise and experience range from collaborating with organizations on their journey to developing and implementing security operating frameworks, Zero Trust, Cloud Security, and Data Protection roadmaps to protecting the security, reliability, and resiliency of information systems supporting mission-critical government and business systems.

Why a Security Culture

What Constitutes a Culture of Security?

Group Discussion

How do you get to a strong culture?

CYBER CULTURE BEGINS AND ENDS WITH OUR *PEOPLE*

ATTACKERS KNOW HOW TO EXPLOIT HUMAN FLAWS:

88% OF DATA BREACHES CAUSED BY EMPLOYEE NEGLIGENCE*

*Source: Stanford University and Tessian Security 2020 (The Psychology of Human Error)

IN THE RACE FOR CYBER RESILIENCE, PEOPLE ARE AT THE CENTER

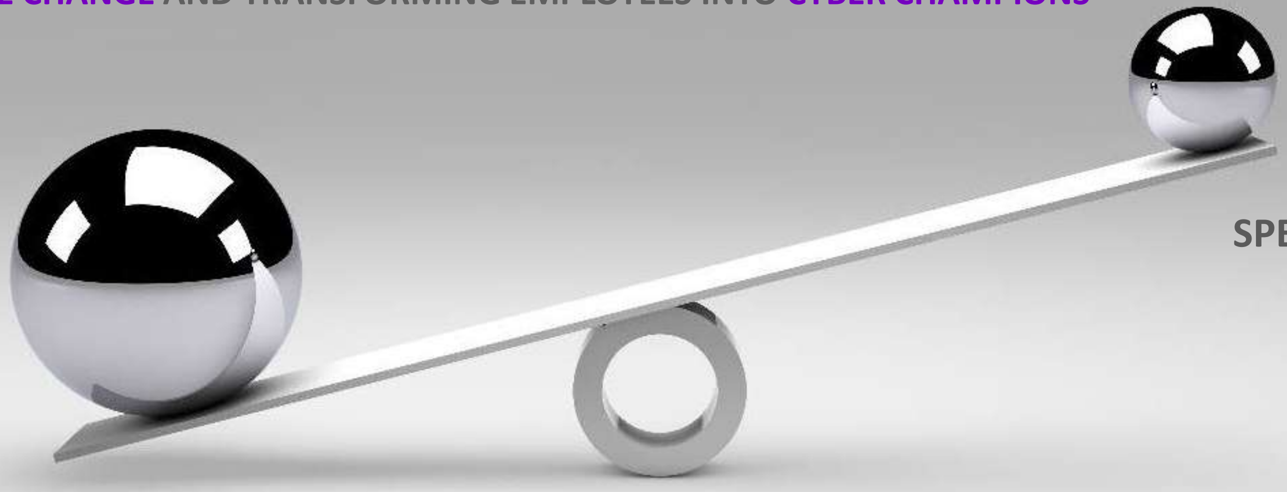
WHAT'S THE ANNUAL COST OF CYBER CRIME?

$6 TRILLION IN 2021

ACCENTURE SEEKS TO **LEVEL THE PLAYING FIELD** AGAINST THREAT ACTORS BY **REDUCING HUMAN RISK** THROUGH **FUNDAMENTAL CULTURE CHANGE** AND TRANSFORMING EMPLOYEES INTO **CYBER CHAMPIONS**

INCIDENTS ATTRIBUTED TO HUMAN FALLIBILITY:

95%



SECURITY SPEND INVESTED IN THE HUMAN FIREWALL:

<5%

TODAY'S CULTURE		TOMORROW'S CULTURE
Security and IT are responsible for cybersecurity	→	**EVERYONE** is responsible for cybersecurity
Only Executives have sensitive information that should be protected	→	**ALL Employees** have information that must be protected
Only businesses can be harmed by cyber threats	→	**ANYONE**, including families, friends, clients, and contractors can be affected by cyber threats
Security is a **Roadblock**	→	**Security is an enabler,** contributes to making IT systems more reliable, resilient, and secure

A CHAIN IS AS STRONG AS ITS WEAKEST LINK…

TRANSFORM YOUR EMPLOYEES INTO YOUR STRONGEST ASSET

BUILD A ‘HUMAN FIREWALL’ THROUGH A CYBERSECURITY PROGRAM THAT FOCUSES ON:

Sponsorship

With vision, **roadmap, sponsorship,** and dedicated budget

ENABLEMENT

Policies and standards to convert knowledge and practice into behaviors that are embedded into ‘ways of working to reduce operational costs, penalties, and breaches.

ENGAGEMENT

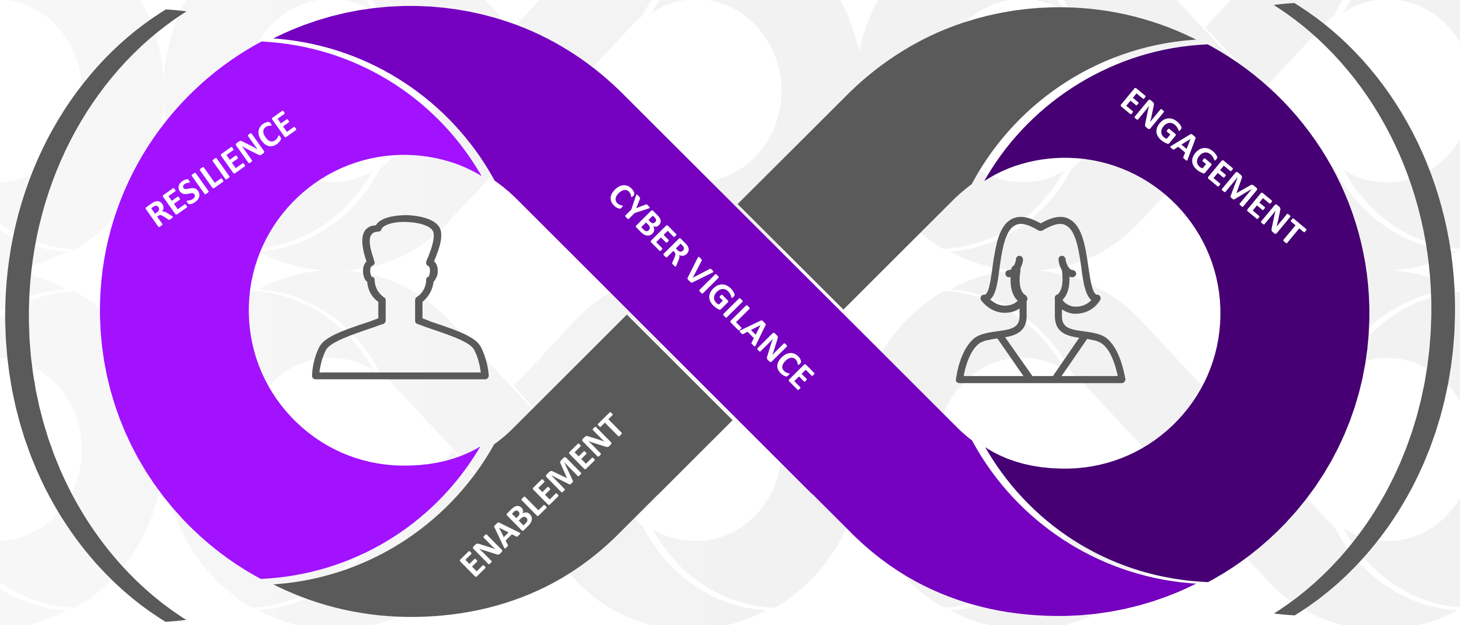
With **compelling and insightful content** that targets relevant threat scenarios to move beyond mere compliance.

CYBER VIGILANCE

With **awareness and understanding** of roles and responsibilities, and clearly defined processes and procedures

RESILIENCE

With a **security-embedded culture** that takes proactive steps in detecting, preventing and resolving suspected or actual incidents



WHEN WE THINK ABOUT BUILDING A HUMAN FIREWALL, WE THINK ABOUT FIVE PILLARS:

1 CYBERSECURE BEHAVIORS AND CULTURE CHANGE

● ●

Transforming the organization wide culture and elevating capabilities to drive ‘security first’ ways of working with insights

- **Behavior Change Programs**, Phishing as-a-Service, & Off the shelf Digital Learning

5 MEASURE & ASSESS

● ●

- Phishing clicks for high-risk individuals (finance, security executives)
- Completion of required and optional trainings
- Number of reported incidents
- Number of security certifications

2 CYBERSKILLS & SPECIALIZED LEARNING

● ●

Educating your Technology and Cybersecurity talent to become more responsive to threat

- Immersive learning w/ **Persona-based (technical audience)** Learning paths
- Digital OT Security Academy, Table-tops and Adversary simulation
- **Orchestrated Roles based Sec Training**

3 CYBERSECURITY TALENT MANAGEMENT

●

Attracting, onboarding, developing and retaining top Cybersecurity Talent to your organization

- Cybersecurity Work & Workforce Strategy, New Skilling and Upskilling
- Sr. Officials Reporting

4 HUMAN-CENTERED CHANGE FOR SECURITY IMPLEMENTATIONS

● ●

Supporting change for Security (Technology, Process) implementations, promoting adoption and embedding change

- Organizational Change Management (OCM) for **Digital Identity, Cloud, IRM, & Compliance Programs**
- Mobilization and Governance

● Build and Transform Services ● Managed Services

How are you doing with **building a strong cyber-culture?**

DISCLAIMER

1. Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology, and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 674,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners, and communities. Visit us at accenture.com.

2. Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions or and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter, or LinkedIn or visit us at accenture.com/security.

3. Accenture, the Accenture logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this presentation and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

- Copyright © 2022 Accenture. All rights reserved. Accenture and its logo are trademarks of Accenture.