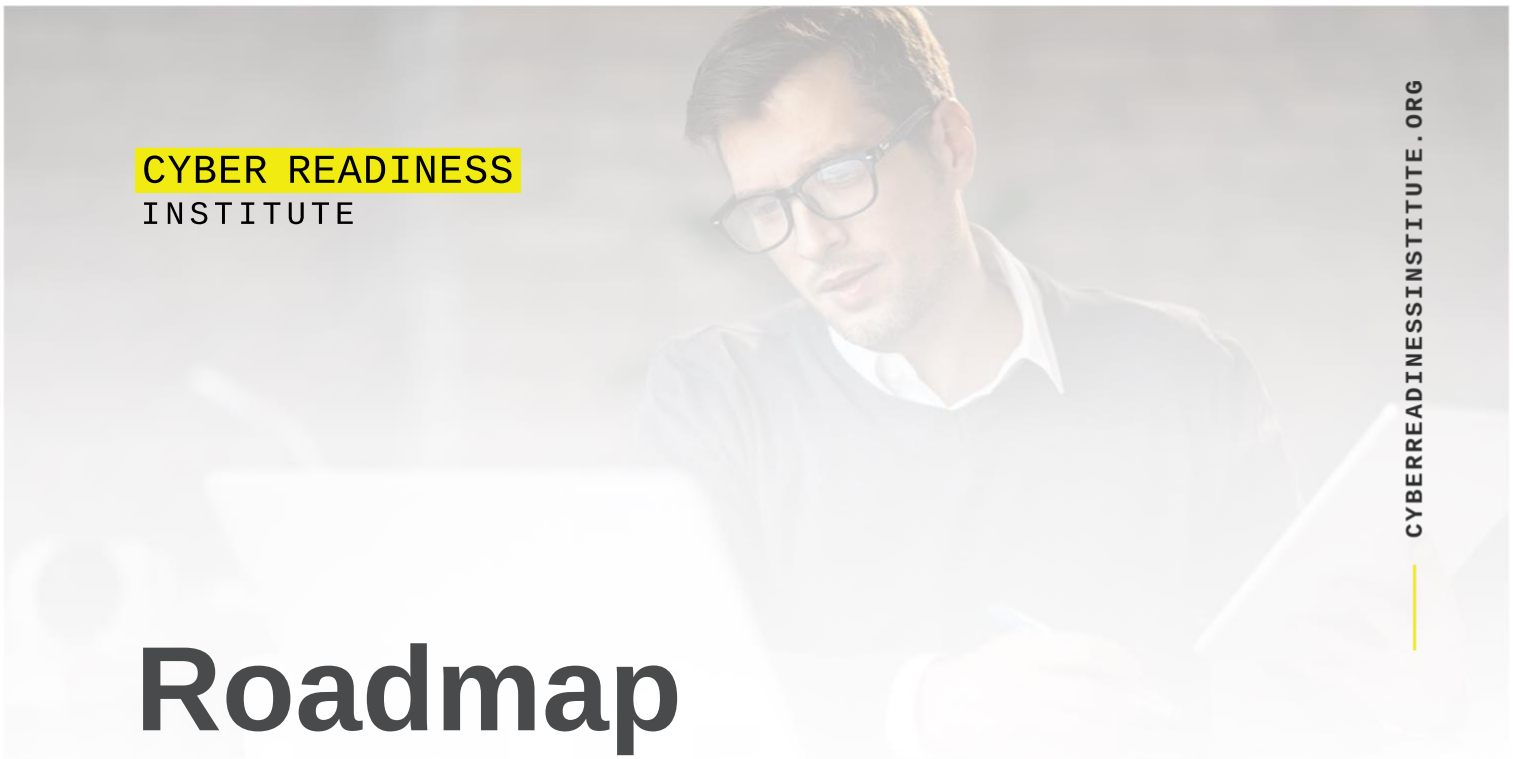


CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG

Roadmap for Preparing Small and Medium-sized Businesses to be Cyber Ready

Table of Contents

Executive Summary

The Cyber Readiness Institute (CRI) has successfully convened senior leaders of global companies to capture best practices for managing the people, processes, and technologies that are foundational for improving cybersecurity. This collaboration has informed the development of content and tools aimed at preparing for, responding to, and recovering from incidents occurring throughout the global community of small and medium-sized businesses (SMBs).

CRI's Co-chairs and members represent multiple business sectors and have a ubiquitous presence around the world. These organizations continue to be at the forefront of helping secure SMBs against cyber threats with their resources, technology, and leadership. Our Co-chairs are Apple, The Center for Global Enterprise (CGE), Mastercard, Microsoft and members are ExxonMobil, General Motors, and Principal Financial Group.

CRI's *Roadmap for Preparing Small and Medium-sized Businesses (SMBs) to be Cyber Ready* looks back on our first five years, gathering insights from data, testimonials, pilot initiatives, content review, and stakeholder engagement to assess our reach and impact. These insights and feedback from discussions with our members and other key participants in the CRI program provided direction for the continuation of specific actions listed below required to accelerate the cyber readiness and resilience of SMBs worldwide. These actions are not standalone efforts but will require coordinated strategies if we are to make significant progress protecting SMBs and their critical role within the global supply chains.

Awareness

Raising the level of awareness and understanding SMBs have about the threats from cyber-attacks related to their continuity of business and the best practices to protect their operations.

1. Global Outreach: Partnering with public and private sector organizations to ensure CRI resources and programs are reaching and being implemented by SMBs all over the world.

2. Data Development and Sharing: Survey, collect, and publish unique, non-vendor sponsored research to identify and encourage the development of solutions that address emerging cyber issues affecting SMBs.

Implementation

Assisting SMBs in the implementation of cyber policies and procedures to create a culture of cyber readiness by focusing on human behavior.

1. Cyber Readiness Standards Establish an international standard for cyber readiness and resilience for SMBs. The CRI Readiness Program can serve as the foundation for an internationally recognized standard implemented and supported by CRI Members and global industries.

2. Global Training Network: Build a global network of qualified Cyber Ready Coaches SMBs can call upon to help create a culture of cyber readiness.

Executive Summary

Continued

Incentives

Developing the tools and methodologies to drive SMBs to improve their business resiliency and cyber readiness.

- Cyber Insurance: Gather insights from SMBs to share with industry by being the authoritative voice for SMBs.
  - Develop guidance for SMBs to select the appropriate coverage for their organization.
  - Assist SMBs to provide documentation of their cyber readiness to adequately address their risk to qualify for a cyber insurance policy.
  - Inform future business models for the insurance markets that can provide incentive for SMBs potentially providing lower rates for being cyber ready.
- Preferred Supplier: Implementing the Cyber Readiness Program with second and third tier suppliers throughout global supply chains for SMBs to gain competitive advantage with their certification.
  - Examine with our members and partners the use of monetary and other financial rewards such as supplier status, to incentivize SMBs to make their operations cyber ready.

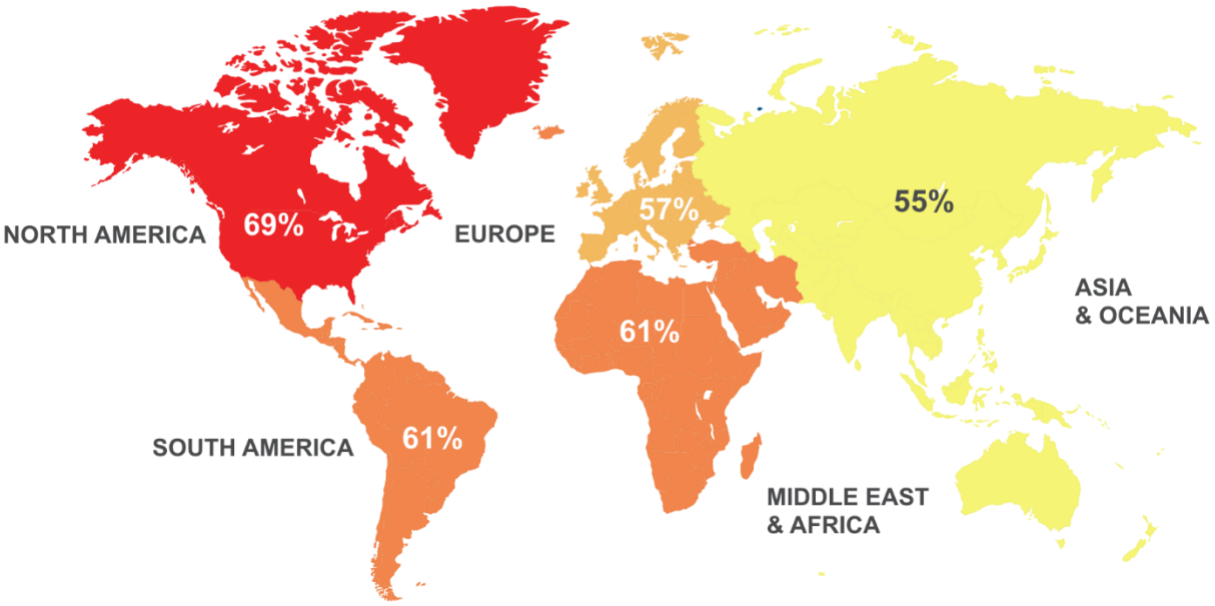
To meet the CRI mission set forth five years ago, we must continue to play a leading role for SMBs as their voice and interpreter on key cyber issues. Continuing to leverage the expertise of our members and partners, CRI intends to emerge as the first stop for SMBs looking to improve their cyber readiness by focusing on human behavior and proven methods and standard technologies to reduce cyberattacks. With many organizations already working to advance these principles, CRI will continue to focus on becoming a global voice for SMBs on key cyber issues, representing their perspective to key decision-makers to ensure their needs are addressed.

CRI would like to acknowledge Apple, GM, Mastercard, Microsoft, ExxonMobil, Principal, and the Center for Global Enterprise for their role in developing this Roadmap. The insights from discussions with representatives from these organizations were vital in shaping CRI's path forward.

Introduction

Cyber Readiness: Why it Matters

% of Companies Who Reported Being Affected by Ransomware



4 in 5

Data breaches due to weak or stolen passwords

*Source: **cidaas***

42%

of small businesses experience a cyber-attack

*Source: **AdvisorSmith***

77%+

More than 77% of organizations don't have an incident response plan; number is likely higher for small business

*Source: **Ponemon Institute / IBM***

Introduction

Continued

According to research from Stanford University, 9 out 10 cyber incidents are due to human error. The Cyber Readiness Institute (CRI)'s approach is founded on the belief that we can change human behavior and the culture of the organization by providing the foundation of strong cybersecurity. It is not necessarily about buying more technology, but rather addressing core issues in combination with changing behavior. Specifically:

- Passwords: 4 in 5 data breaches come from weak or stolen passwords[1]
- Phishing: Just over 1 in 4 employees (26%) said they have fallen for a phishing scam at work in the last 12 months[2]
- Software Updates: 60% of victims said they were breached due to an unpatched known vulnerability where the patch was not applied[3]
- Removable Media/USBs: Threats capable of propagating over USB, or specifically exploiting USB media for initial infection, rose from 19% in 2019 to 52% in 2021[4]

With companies continuing to shift to digital solutions, SMBs will need to improve their cyber readiness and resilience by training their employees to be the first line of defense against these cyber threats to build the culture needed to protect their data, and services and products they offer.

Five Year Review

In 2017, we launched CRI with a focus on providing free content and tools to improve the resilience and cyber readiness of SMBs to secure global value chains. At this natural inflection point, we are evaluating what we have accomplished, and more importantly, defining what still needs to be done to effectively advance the CRI mission and deepen its impact.

While the cyber landscape has shifted dramatically in the past five years, the realities for SMBs are still the same. Lacking resources and managerial bandwidth, these organizations struggle to prioritize cybersecurity and often leave themselves at risk. To examine how to address these foundational issues, we began by reviewing what has been accomplished by CRI thus far. We analyzed program data, partnerships, resources published, and other initiatives.

[1] https://www.verizon.com/business/resources/reports/dbir/
[2] Tessian-Understand The Mistakes That Compromise Your Company's Cybersecurity
[3] Ponemon study on gaps in vulnerability response - ServiceNow
[4] Case Study SMX Pulp and Paper 2 Cybersecurity Honeywell (honeywellforge.ai)

Content and Resources

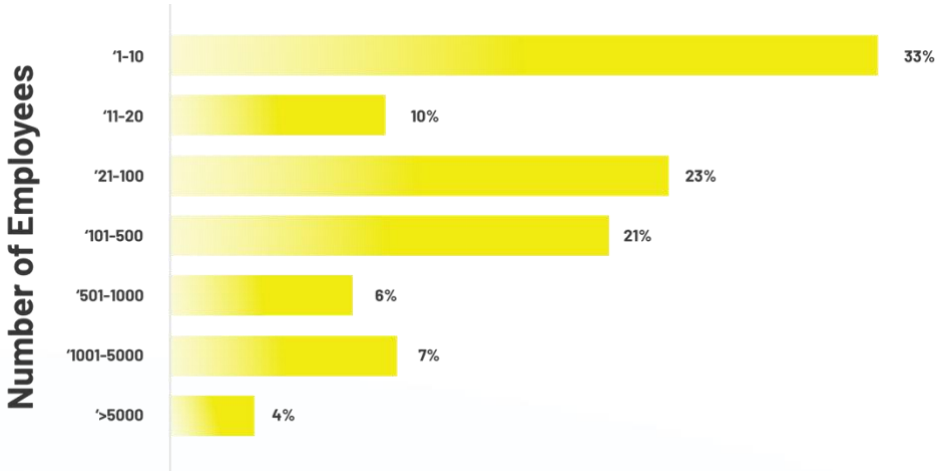
Training Programs

CRI launched the Cyber Readiness Program in 2017 and updated the Program in 2020. The Program focuses on human behavior with information on four key cyber issues to help SMBs develop policies, procedures, and train employees. These "Core Four" issues remain a continued focus because of the impact each can have to improve the security of SMBs.

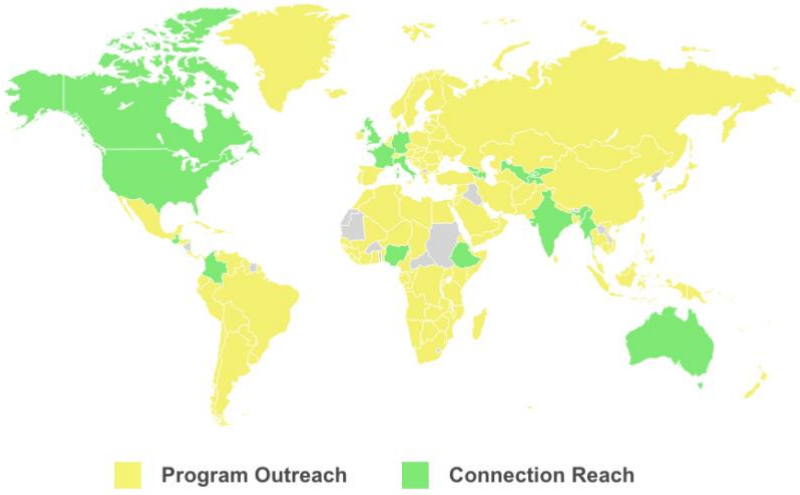
To allow easier accessibility for SMBs around the world, the Cyber Readiness Program has been translated into Spanish, Portuguese, and Russian. Prior versions of the program have been translated into French, Arabic, and Japanese.

In October 2020, CRI extended the Cyber Readiness Program with the Cyber Leader Certification Program. It is a management program focused on enhancing the ability of individuals at SMBs to create and sustain a cyber-ready culture in their organization. This more in-depth program teaches the designated Cyber Leader how to manage the people, processes, and technology critical to securing their organization.

Cyber Readiness Program Enrollments



Global Reach of CRI's Program Enrollment and Partnerships



To date, enrollment for CRI's programs has reached almost 5,000 SMBs in 178 countries representing over ninety industry sectors. The above map depicts the global reach of CRI's program enrollment and partnerships where SMBs have directly engaged with our resources on the CRI website (yellow) and where our partner organizations have directly engaged with SMBs to assist with implementation of our programs (green). Most enrollments representing SMBs are organizations with less than 100 employees.

Guides

Since 2017, CRI has released 25 guides for SMBs on topics such as multifactor authentication (MFA), managed service providers (MSPs), telehealth, ransomware, hybrid work, and many more. These guides serve as easily digestible resources on topics where SMBs have knowledge gaps.

Social Media

CRI's unique content and resources posted on Twitter, LinkedIn, Facebook, YouTube and Instagram have reached over seven million people, generating close to 350,000 engagements, and bringing 118,000 people to the website for more information.

These accomplishments are just a part of CRI's work in the past five years and have provided clear insights on where to go next. For example, only 28% of the almost 5,000 SMBs enrolled have completed our programs due to low awareness, lack of implementation guidance, and proper incentives. CRI will continue to tackle these challenges to bolster the adoption of policies and procedures that are available for their improved security.

CRI Roadmap

With SMBs accounting for nearly 99% of firms in Organization for Economic Cooperation and Development (OCED) countries,[5] the actions outlined in the sections to follow will strengthen global supply chains by addressing basic knowledge and resource gaps to create a more cyber ready and resilient network of SMBs globally.

CRI views the road to improving the cyber readiness and resiliency of SMBs globally along three paths: Awareness, Implementation, and Incentives, which are not to be viewed as standalone actions but will require coordinated strategies including both public and private organizations to make significant progress to assist SMBs.

Awareness

One issue that continued to arise in discussions with stakeholders was the overall lack of awareness surrounding the risk SMBs face without basic cyber policies and procedures. A recent CNBC survey found that over half of small business owners surveyed were not concerned their business will be the victim of a cyberattack[6]. This response makes clear that a large knowledge gap exists. Understandably, as most SMBs focus on the day-to-day work required to run a business with limited resources, they are left with little time to catch up on the latest cyber breach or review preferred best practices. Therefore, CRI has an opportunity and market permission to establish itself as the "go to source" on cybersecurity for SMBs, with *free* resources focused on topical cyber issues all in one place. Leveraging strong partnerships with private and public organizations, CRI will use original research to focus on timely issues such as our recent survey on MFA. This will provide unbiased information to improve awareness of cyber issues afflicting SMBs.

Global Outreach

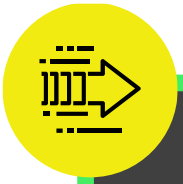
Future awareness campaigns and targeted outreach must continue to focus on SMBs outside of North America. This international focus aligns with the global nature of digital supply chains and provides insights into the realities of operating in different regions. Getting resources into the hands of more SMBs in Africa and South America will raise global awareness on the issues of cyber readiness and resilience. To effectively reach these regions, CRI will target recruitment and partnership efforts with the appropriate organizations and SMBs operating in these countries. This representation will provide new perspectives to our current resource development process and help CRI effectively message to different cultures. The continued translation of CRI's training programs and other resources is key to the

[5] https://www.oecd.org/mcm/documents/C-MIN-2017-8-EN.pdf
[6] CNBC|SurveyMonkey Small Business Index Q2 2022

success of this global outreach. Future translation efforts will be guided by our members and partners, allowing CRI to raise awareness of cybersecurity issues around the world.

Data Development and Sharing

SMBs are focused on their businesses and often fail to understand the consequences ignoring basic cyber hygiene can have on their business. Even when SMBs and other professionals in the cybersecurity industry seek out data they often find themselves with results from vendors trying to sell a product. Reinforcing CRI's credential as an independent, trusted source of data will assist the cybersecurity industry to develop solutions for SMBs. By collecting unique data from our programs, conducting surveys, and leveraging the resources of our members and partners, CRI will be able to better quantify and communicate the effect of a cyber event to SMBs.



Implementation

Offering SMBs resources to improve their cyber readiness is only part of the challenge. Employees are becoming more aware of how their behavior impacts security, with 36% of employees believing they have made a mistake at work that has compromised security in the last 12 months[7]. Still, they fail to learn how to avoid making the same mistake without proper policies and training. Understanding the challenges SMBs face, CRI must create mechanisms to improve cyber readiness without creating confusion, unnecessary work or draining resources. With the completion of pilot initiatives with our members and partners, we designed a unique model – a high-touch, step-by-step approach as the most effective way to get SMBs to complete the Cyber Readiness Program which incorporates key features of company-specific cyber policies and procedures, and incident response plans. CRI plans to expand this capability, offering close engagement to global supply chain leaders and SMBs as they work to improve their cyber security with a baseline standard and a global network of qualified Cyber Coaches.

Cyber Readiness Standards

As standards, regulations, technologies, and other key aspects of cybersecurity move at a break-neck pace, the majority of SMBs are not equipped to keep up. But do they need to? And at what cost? Instead, CRI is working with public and private institutions to establish a baseline set of policies and procedures SMBs can implement to prove their cyber readiness. These policies would give SMBs an internationally recognized starting point in their journey, something they often struggle to find. Once met, the CRI standard will provide customers, supply chain partners, insurers, and other interested parties with assurance that a business is cyber ready. Developing these policies and procedures require strong public and private collaboration, as well as direct input from SMBs to ensure their feasibility and effectiveness. CRI's current Cyber Readiness Program and the associated certification process is already serving as a starting point for a scalable process in which SMBs can work with CRI approved Cyber Coaches. As the standard evolves over time, we will look to expand our programs and materials to other topics such as vulnerability management, and topics identified as vital to improving the cybersecurity of SMBs.

---

[7] Understand The Mistakes That Compromise Your Company's Cybersecurity

Global Training Network

To increase completion rates and overall program effectiveness, CRI intends to work with members and other organizations to develop a global network of qualified Cyber Coaches. Modeled on a successful partnership with Cyber Hawaii, CRI will train individuals in local geographic areas to help SMBs work through their cyber readiness journey and verify their successful completion of their program. This localized support network will help CRI customize the needs of SMBs, allowing for global partners to work through CRI's Programs at their own pace. This approach serves two purposes, assisting SMBs through the program and externally verifying program completion for CRI to award certification. The development of this network will build the cyber workforce and expand the resource pool for future initiatives. Additionally, we see the development of this network as incentive for SMBs knowing they don't have to go it alone.

Incentives

Raising awareness and offering implementation support is necessary but not sufficient to help SMBs invest in their readiness and sustain their resilience. Financial incentives and possibly disincentives, have proven effective mechanisms to affect cyber practices and procedure. A 2021 survey conducted by CRI found only 21% of SMBs are confident that the time and money their organization invests in cybersecurity will decrease their risk.[8] As we look to improve the cyber readiness of SMBs, we must offer new approaches to greater security and brand protection. Global organizations and governments need to play a part requiring their suppliers and partners to implement features such as MFA.

Cyber Insurance

SMBs do not typically have the people, processes, and technologies to develop the robust security programs required to qualify for cyber insurance. Nor do many underwriters and insurers have proper visibility into the realities of running a small business. This has created a confusing situation for both insurers and those SMBs seeking the appropriate policy for their needs. To clear up this confusion, CRI is leveraging our ability to convene stakeholders to identify the knowledge gaps, develop material to fill them, and create incentives for SMBs. Accomplishing this will require CRI to provide SMBs with guidance selecting appropriate policies and work with insurers to craft discounts or other financial incentives to encourage SMBs to adopt strong cyber practices.

Preferred Supplier Status

Global supply chain leaders must recognize the role they can play to ensure their suppliers are cyber ready. CRI will collaborate with our members and partners to help establish a preferred supplier status for second- and third-tier suppliers that demonstrate they have taken appropriate steps to become cyber ready. CRI will work with SMBs to assist them in achieving that preferred supplier status. Additionally, CRI will work with organizations to examine if offering monetary incentives can increase adoption of this cyber readiness standard.

Looking Ahead

This Roadmap outlines three paths where all organizations — private or public — must do their part to improve the cyber readiness and resilience of their partners and suppliers. CRI, our members, and partners intend to follow through on our part to achieve this outcome with global SMBs. In planning for the next five years, it is important to acknowledge the scale of the current issues facing not just SMBs, but public and private organizations in all regions, industry sectors, and sizes. CRI believes the road to success is paved on the principles of strong partnerships, workforce development and retention, and accessible behavioral and technological solutions.

Partnerships

Public and Private institutions around the world need to open the lines of communication with an enhanced focus on collaboration, not competition. Sharing data, best practices, effective policies, and lessons learned is key to improving the overall ecosystem for SMBs.

Workforce Development and Retention

As countries address growing the global cybersecurity workforce, there will be a larger talent pool available that will benefit SMBs and large organizations. When done properly, there will be more cyber capable employees employed by SMBs. CRI plans to do its part to provide the foundational knowledge as this workforce continues to grow to ensure continuity and resiliency in global business operations.

Accessible Solutions

SMBs benefit greatly from advancing user-friendly and affordable tools and systems for managing risk. Developing these technologies and behavioral solutions will require investments focusing on the real cybersecurity needs of SMBs, and not another feature to sell them.

CRI will continue to focus on becoming a voice for SMBs globally on critical cyber issues, representing their perspective with key decision makers to ensure their needs are considered.

Co-Chairs and Members

CRI's Co-Chairs represent multiple global business sectors and continue to work with CRI and other organizations to help secure SMBs against cyber threats. Their contributions since CRI's inception are innumerable, but some notable work includes:

Apple

Sponsored a CRI Pilot Program to improve the security of their SMB suppliers.

The Center for Global Enterprise

Launched the Digital Supply Chain Institute (DSCI) to focus on the evolution of enterprise supply chains and the practical application of supply chain management best practices including risk management and cybersecurity.

Mastercard

Established the Trust Center to share information, tools, and resources to help businesses improve their cybersecurity.

Microsoft

Released Microsoft Defender for Business to provide SMBs endpoint detection and response capabilities to protect against ransomware and other sophisticated cyber threats.

CRI's members, ExxonMobil, and Principal Financial Group have also played a significant role in furthering CRI's mission and GM conducted a Pilot Program with their critical suppliers. Our members provide direct feedback on content development and program improvements.