RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PNG-T08**

Supply Chain Cyber Readiness: Upping Your Game

MODERATOR: **Christine Pelione**
Cybersecurity Strategic Planning
General Motors

PANELISTS: **Michele A. Brown**
Director, Third Party Cybersecurity
General Motors

Monty R. McGee
Associate Director
Cyber Readiness Institute
@Cyber_Readiness

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA® Conference, RSA Security LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAConference2022

MODERATOR:

Christine Pelione
Cybersecurity Strategic Planning
General Motors

PANELISTS:

Michele A. Brown
Director, Third Party Cybersecurity
General Motors

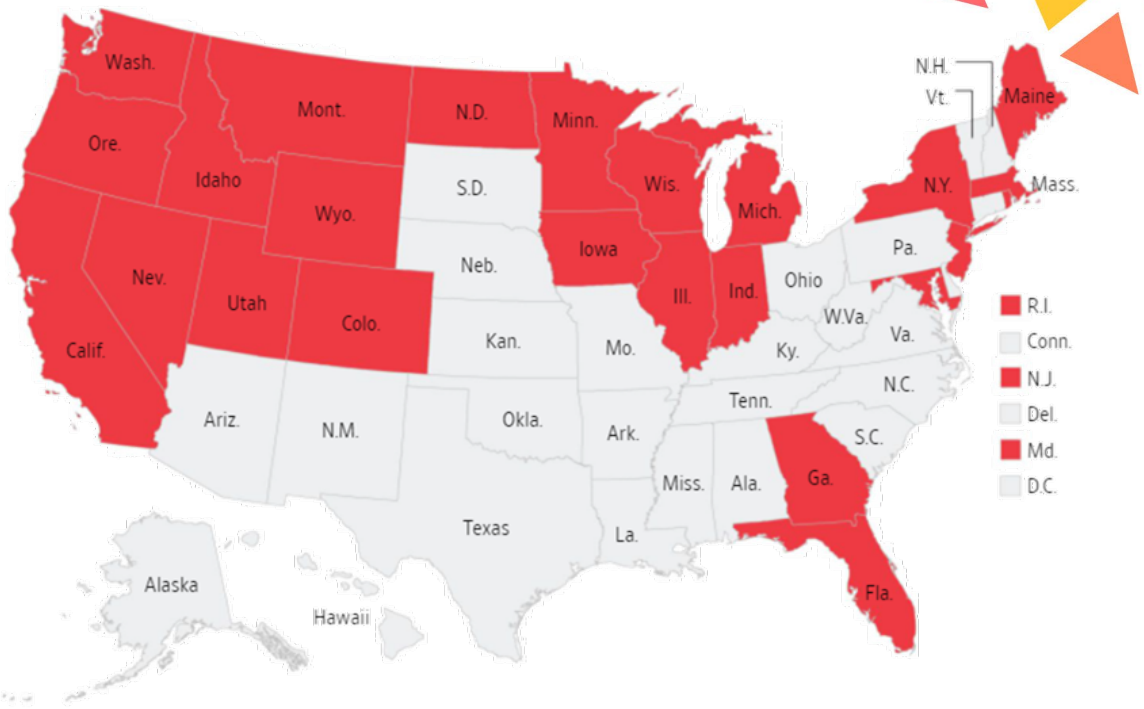
Monty R. McGee
Associate Director
Cyber Readiness Institute
@Cyber_Readiness

RSAConference2022

Scene Setter

How many similar stories have you heard this year?

An Ordinary Day…or is it?



An Attack on One is an Attack on All

Hackers seeking to infiltrate the power grid targeted companies operating in at least 24 states, Canada, & the U.K.

CYBER READINESS INSTITUTE

https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112

Why It Matters

- **4** in **5** data breaches come from **weak or stolen passwords**

https://www.cidaas.com/world-wide-4-out-of-5-data-breaches-arise-from-weak-or-stolen-passwords/

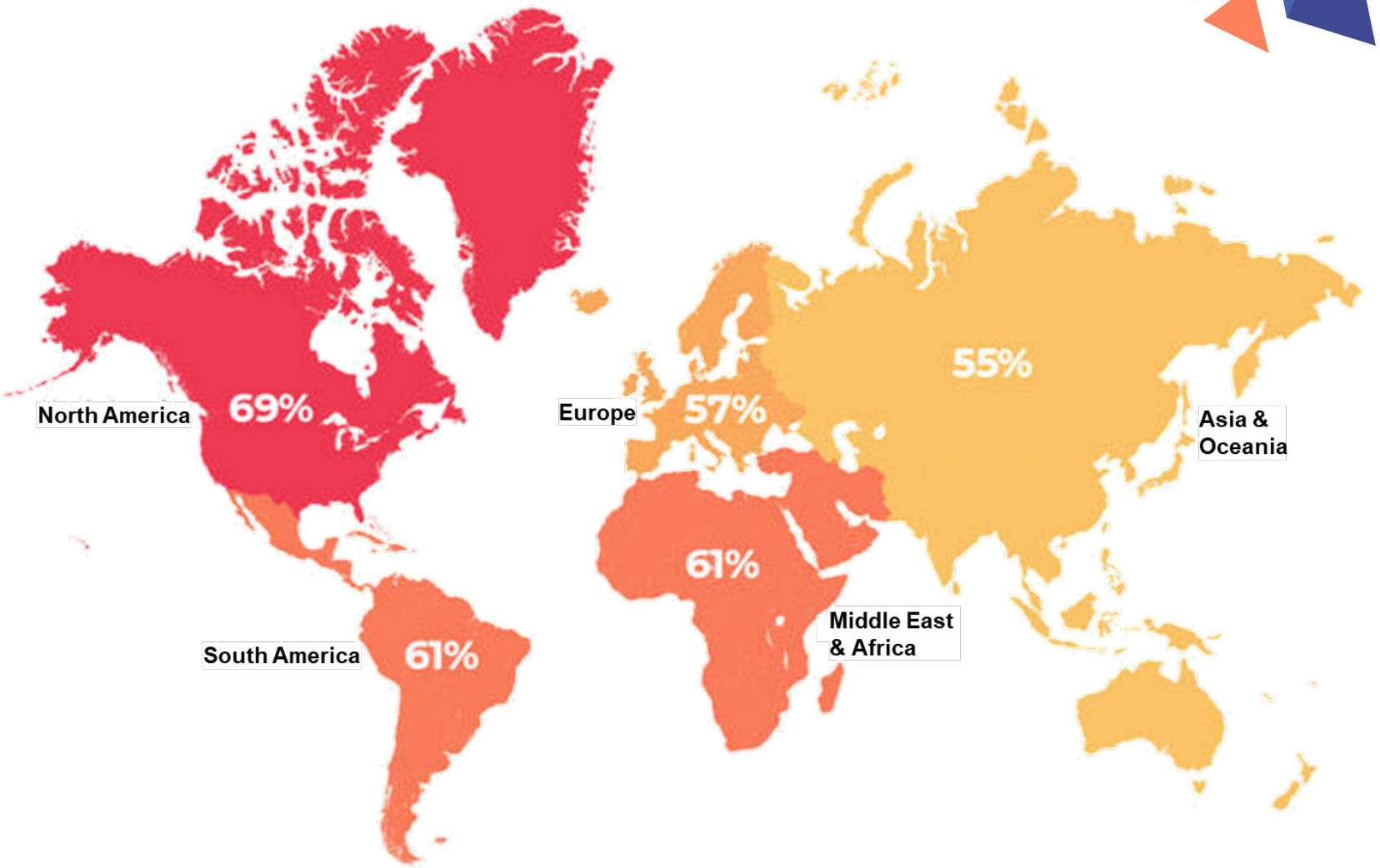
- **42%** of **small businesses** experience a cyber-attack

https://advisorsmith.com/data/small-business-cybersecurity-statistics/

- More than **77%** of organizations don't have an **incident response plan**;

number is likely higher for small business.

https://www.sdxcentral.com/articles/news/ibm-77-of-enterprises-dont-have-a-cybersecurity-incident-response-plan/2019/04/



% of Companies Who Reported Being Affected by Ransomware

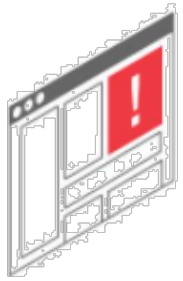
https://www.techrepublic.com/article/infographic-ransomware-attacks-by-industry-continent-and-more/

CYBER READINESS INSTITUTE

Hackers stole employee credentials to gain access to corporate systems.

Tools of the Trade

They **sent emails** with malicious links or attachments that helped **steal the recipient's credentials**.



They planted malicious code on **trusted websites** that they hoped their targets would visit. The code **recorded visitors' confidential info**.

With stolen credentials, hackers used virtual private networks and remote desktop programs to **stay hidden** and **maintain access** to internal networks.

CYBER READINESS INSTITUTE

RSAConference2022

You CAN avoid this…

The Cyber Readiness Institute can help you Up Your Game today!

Why It Matters

www.becyberready.com

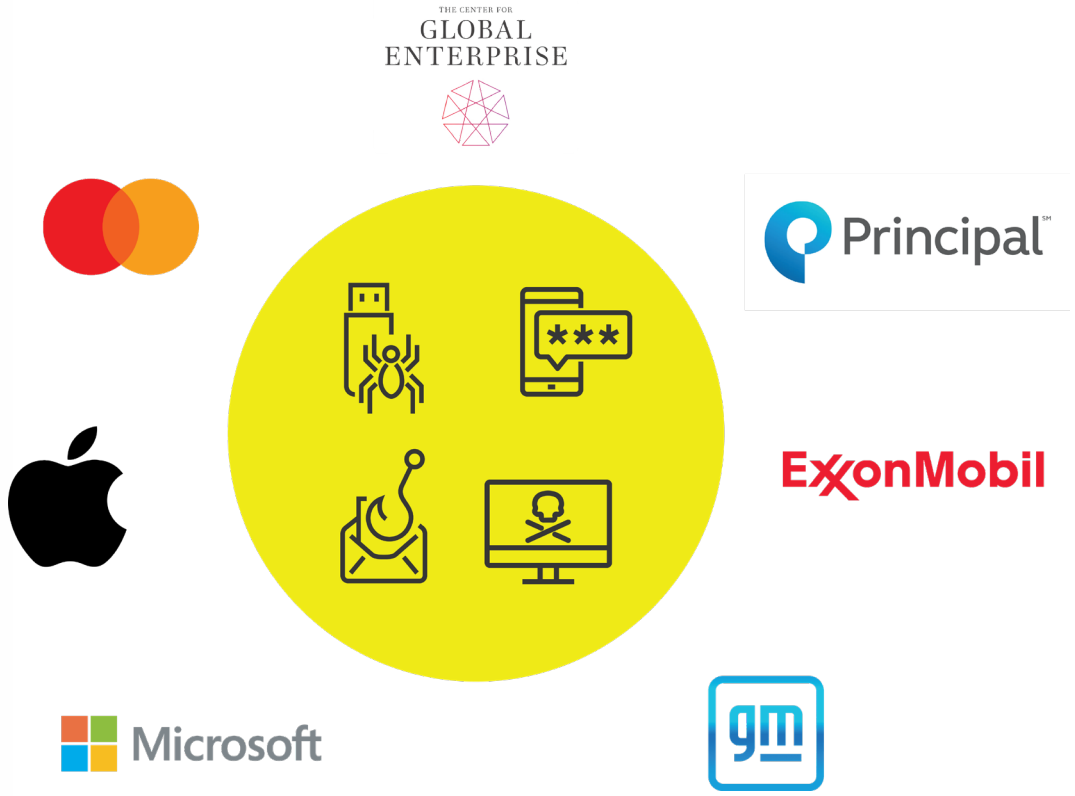
Nearly **9** in **10** security breaches are caused wholly or in part from

human error

(Stanford University)

The Cyber Readiness Institute

- Global non-profit focused on enhancing cyber readiness of small & medium businesses (SMBs)
- Convenes senior leaders of global companies and value chain partners to strengthen global supply chain security
- Develops ***free*** content & resources that reach more than 2 million SMBs worldwide



CYBER READINESS INSTITUTE

The Cyber Readiness Institute Approach

- Focus on human behavior to create resiliency and a culture of cyber readiness
  - Empower individuals/employees on role in cybersecurity
  - Develop good cyber habits among SMBs
  - Strengthen the security of global supply chains
- Provide free, self-guided, online cybersecurity tools and resources

Cyber Readiness Program

- Comprehensive, self-guided cyber training for SMBs

Cyber Leader Certification Program

- Personal professional credential for the Cyber Leader

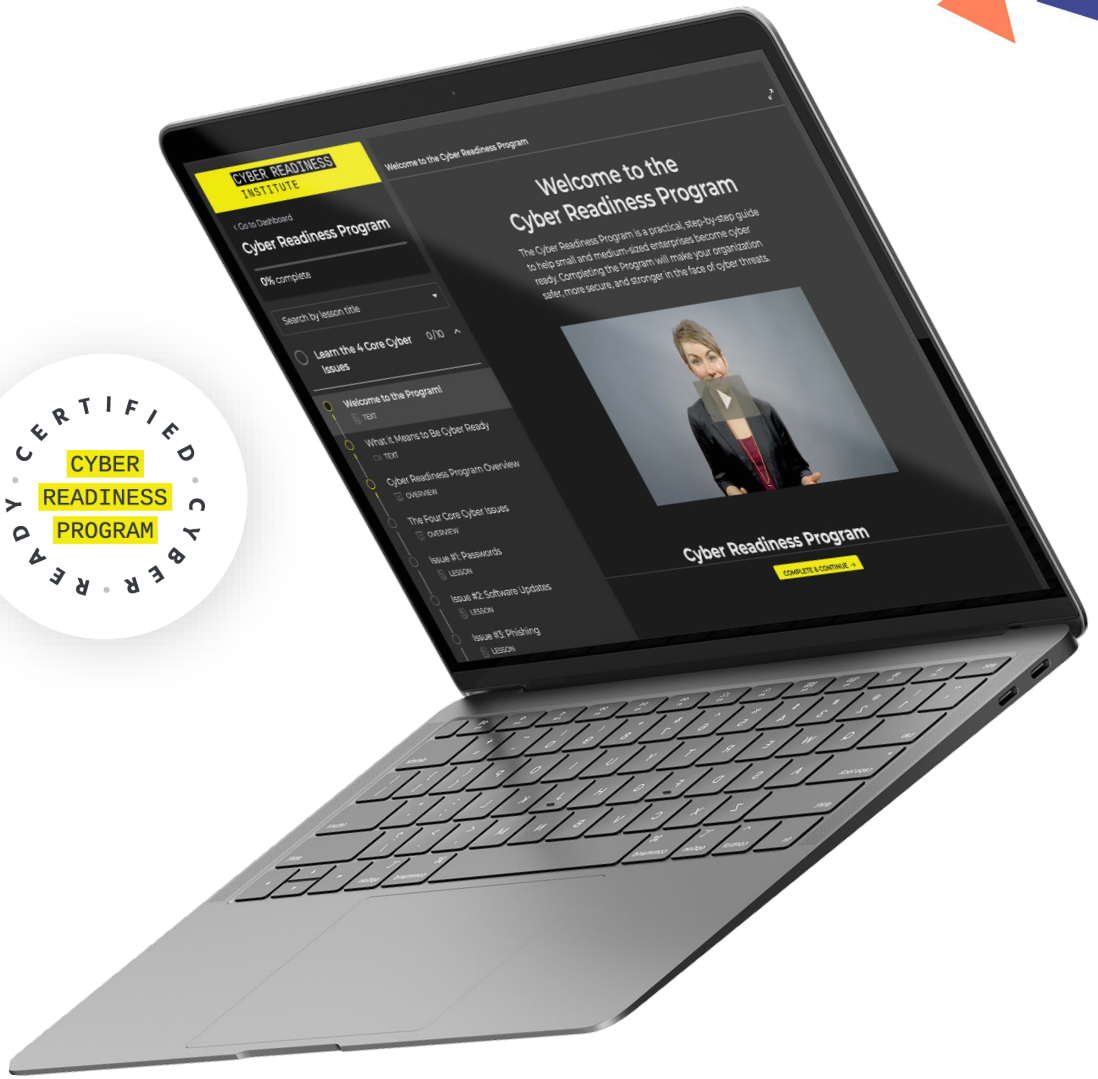
Quick Reference Guides

- Remote and Hybrid Work Environments, Ransomware Playbook, Telehealth, and Cloud FAQ

CYBER READINESS INSTITUTE

The Cyber Readiness Program

- Focus on "Core Four" issues for cultural change
  - Passwords
  - Software Updates
  - Phishing
  - USB Use
- Create and communicate Cyber Readiness Playbook with practical policies and incident response plan
- Measure impact through baseline metrics and reassessment

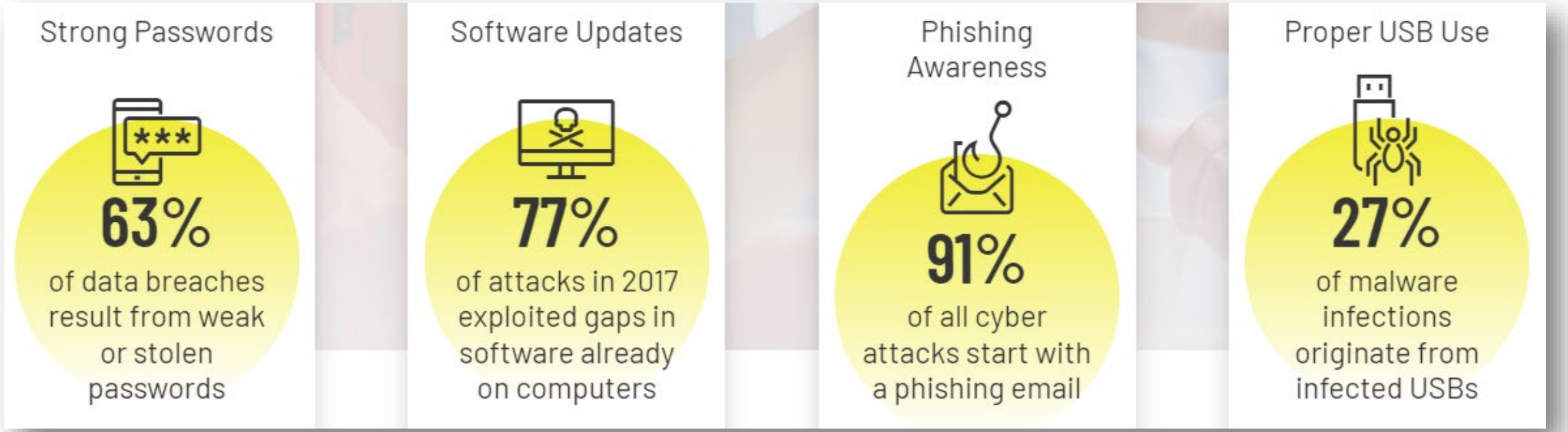


CYBER READINESS INSTITUTE

www.BeCyberReady.com

CYBER READINESS INSTITUTE

You can start with 4 Core Areas…



According to Microsoft, **99.9%** of account compromise attacks can be **blocked simply by using MFA**.

CYBER READINESS INSTITUTE

RSAConference2022

Explained: General Motors' Supply Chain Security Pilot

GM, with CRI, launched a supply chain security pilot focused on enhancing its suppliers' cyber readiness.

General Motors' Supply Chain Security Pilot

ting the Context

- Vast third-party ecosystem
- Global presence
- Ranging in size
- Rapidly evolving threat landscape
- Varying levels of Security posture

Leveraging CRI

- Proven platform and capability
- Free resource
- 67% of the out-of-the-box content aligned to GM standards
- Win-Win!

Customizing for GM

- Enhanced the content
- Added a certification
- Created a dedicated site
- Defined maturity measures

330+

Invitations

40%

Engagement

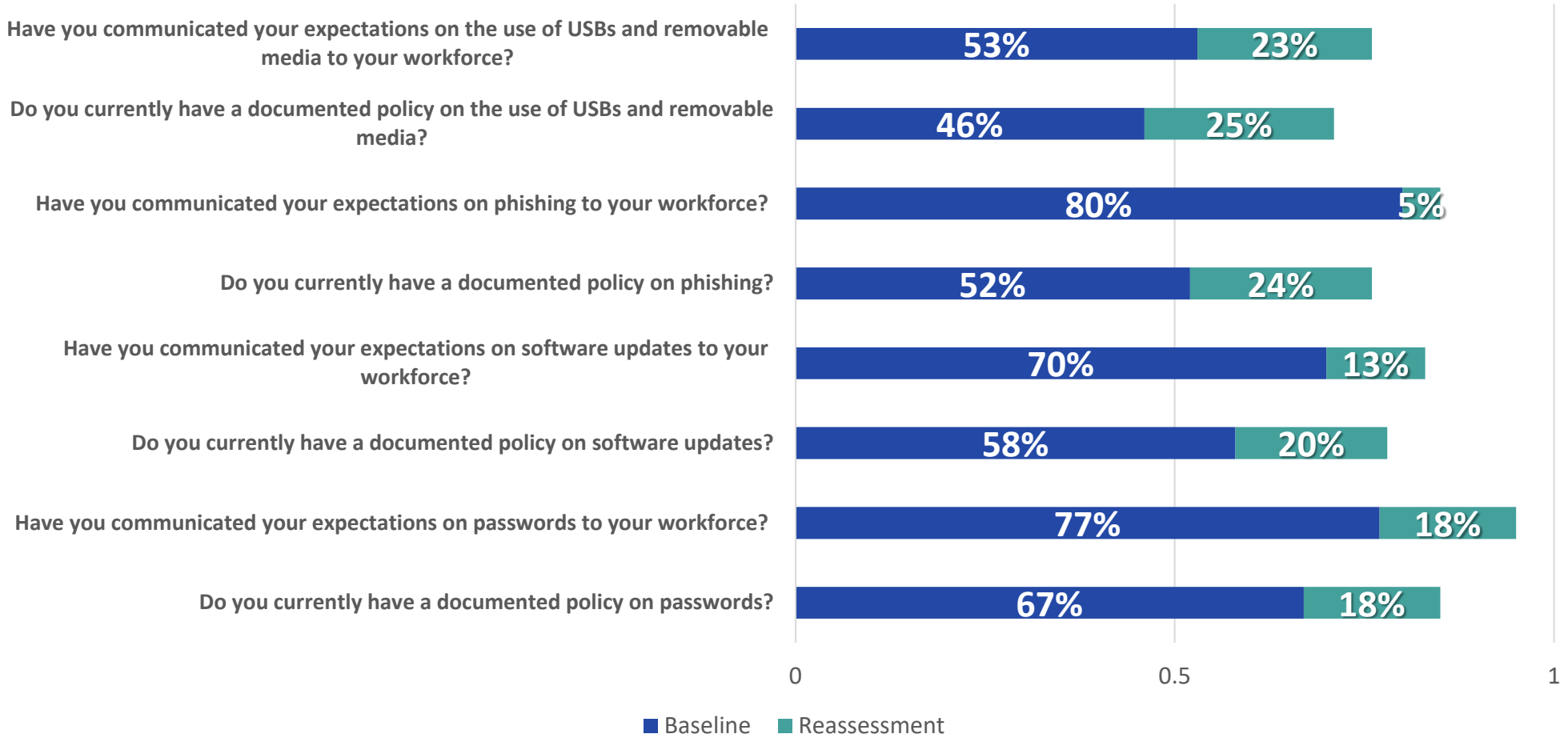
18%

Completion

CYBER READINESS INSTITUTE

General Motors' Supply Chain Security Pilot

Initial Results: Significant Improvement in Overall Security Posture*

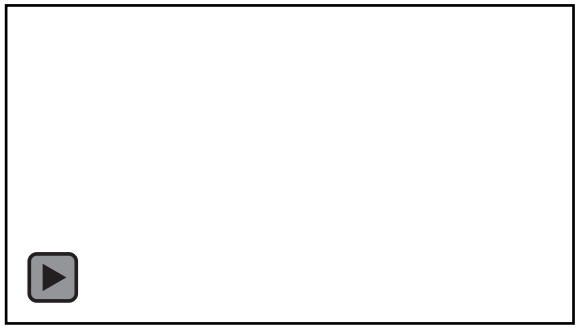


CYBER READINESS INSTITUTE

*Results based on survey responses elicited before and after completing the Cyber Readiness Program

General Motors' Supply Chain Security Pilot

Participant Verbatims



- *"Easy to follow actionable & focused plan. It will help our organization stay cybersecurity aware at all times. Wish the program was available in more languages."*
- *We will focus on letting employees have more information security knowledge and remind them at any time."*
- *"Although our company has been doing information security management, this training has more systematically and theoretically improved my understanding of information security management and will soon affect our employees. Thank you very much."*
- *"Helping to quickly identify key areas we are most at risk and providing resources to help bridge those gaps. Thank you."*
- *"This course has shown us how to break down cyber readiness into knowledgeable steps for all of our employees to follow and understand."*
- *"This program allows us to verify or reinforce our processes and procedures to increase the security controls of policy compliance and cybersecurity assessments."*

CYBER READINESS INSTITUTE

Cyber Readiness By the Numbers

93% users that complete the Cyber Readiness Program say it had a moderate, high, or very high impact on the cyber readiness of their organization.

CRI content is accessed by users in **161 countries.**

CRI's network reaches **over 2M SMBs, globally.**

Apply What You Have Learned Today

- Next week you should:
  - Check out BeCyberReady.com for more tips, practical guides, and useful training.
- In the first three months following this presentation you should:
  - Host a leadership discussion about how your organization can illuminate the cyber readiness of your suppliers and partners.
  - Consider partnering with an organization like CRI to help you Up Your Game.
- Within six months you should:
  - Draft and begin implementing a plan for your own supply chain pilot
  - Contact CRI at info@cyberreadinessinstitute.org for guidance on using *free* resources in your pilot.

Michele Brown
General Motors
michele.a.brown@gm.com

Monty McGee
Cyber Readiness Institute
mmcgee@cyberreadinessinstitute.org

Christine Pelione
General Motors
christine.pelione@gm.com

CYBER READINESS INSTITUTE

Thank You