AGC 2020 CONVENTION The Construction Association

PREPARING FOR THE INDUSTRY OF TOMORROW

Cyber risks in the construction industry: Are you prepared?

The following CE credits are offered for this session:

0.1 IACET CEU | The Associated General Contractors of America (AGC) has been accredited as an Accredited Provider by The International Association for Continuing Education and Training (IACET). In obtaining this accreditation, AGC has demonstrated that it complies with the ANSI/IACET Standard which is recognized internationally as a standard of good practice. As a result of their Accredited Provider status, AGC is authorized to offer IACET CEUs for its programs that qualify under the ANSI/IACET Standard.

1.0 AIC CPD Credit | AGC of America has been approved to offer Continuing Professional Development (CPD) credits for qualifying programs by the American Institute of Constructors (AIC).

1.0 SMPS CEU Credit | AGC of America is approved by the Society for Marketing Professional Services (SMPS) to offer SMPS CEUs.

1.0 AIA Learning Unit (LU) | The Associated General Contractors of America is a registered provider of AIA-approved continuing education under Provider Number G523. All registered AIA CES Providers must comply with the AIA Standards for Continuing Education Programs.

AGC of America is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.

This session is designated for **1.2 CPE credits** in the field of Information Technology.

How to earn CE hours for this session

Participants must:

1. Check in with attendance scanner at the door or in the back of the room.
2. Attend at least 95% of the session.
3. Complete the session and post-program evaluation.
4. Complete a brief assessment with a score of 75% or greater.

Additional instructions will be emailed to attendees requesting CE credits.

For those seeking AIA credits, please provide your AIA number so we can report your attendance. You may contact **Jo-Anne Torres**, Manager of Professional Development and Continuing Education, at **jo-anne.torres@agc.org** or call (703) 837-5360 for questions.

Learning Objectives

By the end of this session, participants will be able to:

1. Examine cyber risk activity in the construction industry.
2. Identify the most common cyber security risks.
3. Discuss ways to help protect your organization from cyberattacks.
4. Explore how an information security management system (SMS) can help you develop effective and robust cyber security for your organization.

Karen Reutter

Head of Construction,
Zurich North America

Michelle Chia

Head of Professional Liability and Cyber,
Zurich North America

Nikki Ingram

CISSP, Cybersecurity Risk Engineering,
The Zurich Services Corporation

Cyber basics

Terminology

Cyber	Having to do with a computer or a computing system
IoT	"Internet of Things" relates to any device that can be connected to the internet.
Threat	Any circumstance or event with the potential to cause harm to an information system. Related terms: Threat actor = Bad guy Threat vector = Modus operandi
Vulnerability	Any condition that leaves an information system open to a threat
Exploitation	The successful execution of a threat via a present vulnerability
Risk	A relative measure based on the likelihood of an exploitation and the resulting impact of the adverse event on the organization

Key exposures: Statistics to consider

243

Median number of days advanced attacks are on the network before being detected

Mandiant

70%

Percentage of breaches associated with nation-state or state-affiliated actors involved phishing

2018 Verizon Data Breach Investigations Report

2.9 billion

Records leaked in 2017 (this only counts publicly-disclosed breaches)

IBM 2018Cyber Security Intelligence Index

23%

Percentage of users who share their network passwords with colleagues

IS Decisions - FROM Brutus to Snowden

28%

Likelihood of a recurring material breach over the next two years

2018 Cost of Data Breach Study; Global Overview, Ponemon

10%

Percentage of email credentials of Fortune 500 employees on the dark web

2018 Vericlouds

Common passwords

"123456," "password," "!@#$%^&," "qwerty," "12345," "123456789," "aa123456," "1234567," "football," "iloveyou," "admin," "letmein," "starwars," "login," "abc123," "monkey," "654321," "dragon," "Password123"

Splashdata 2019

$148

Average cost per lost or stolen record

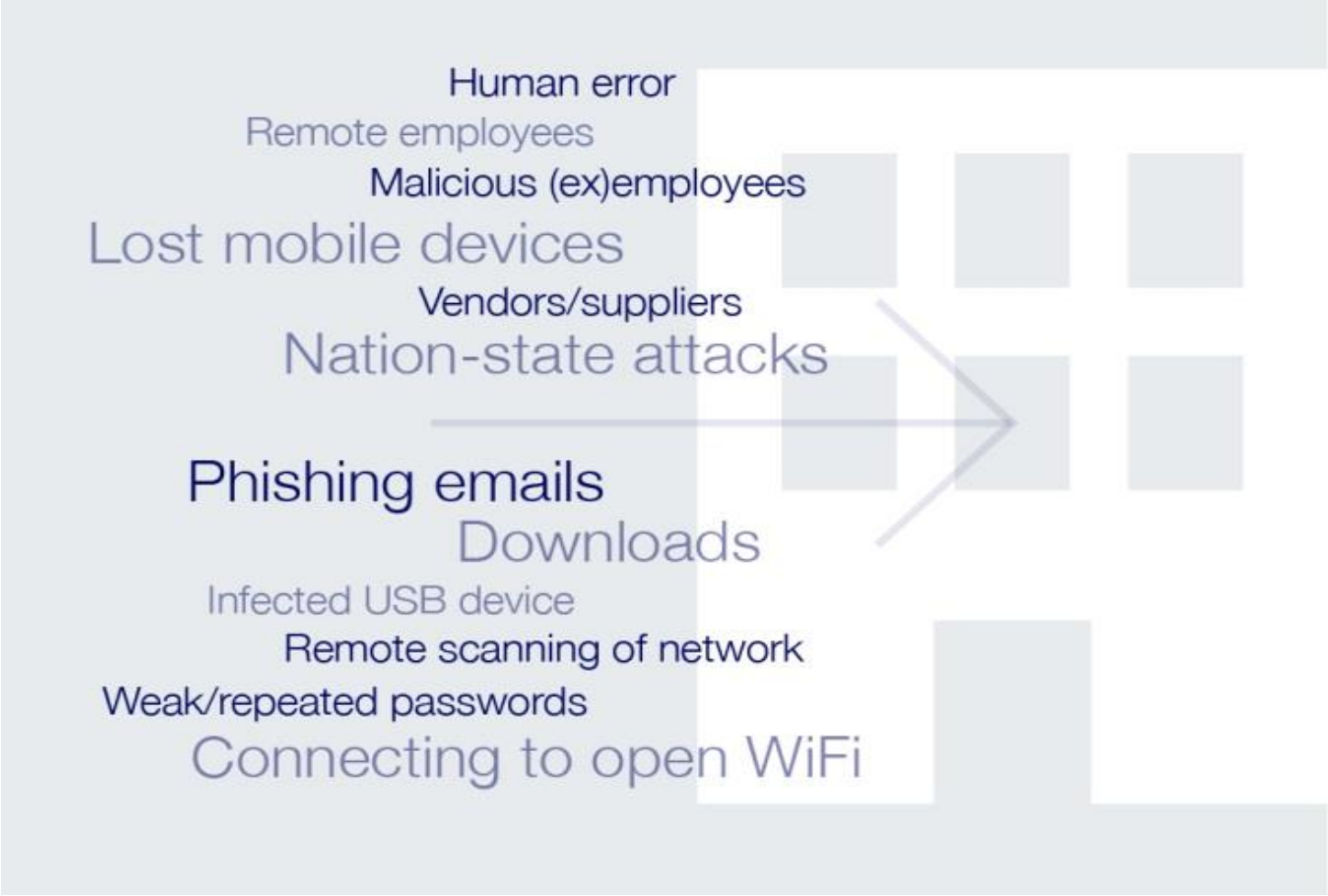
2018 Cost of Data Breach Study; Global Overview, Ponemon

58%

Percentage of victims categorized as small businesses

2018 Verizon Data Breach Investigations Report

Cyberthreats: Threat Sources



Cyberthreats: Threat Sources

Cyberthreats: Types of attacks

Cyberthreats: Risk Consequences

Mitigating cyber threats: Where to start

- Accept that you have something that is valued by others and that you are a target, regardless of your size
- Promote a cyber-risk management culture and thoughtfulness
- Know what you are protecting
- Keep up with patching
- Encrypt whenever possible
- Control access, especially privileged access
- Expect and prepare for a cyber event
- IDENTIFY, PROTECT, DETECT, RESPOND and RECOVER

The future of cyber risk: 5 key considerations

- **Frequency:** Cyber events will continue to increase.
- **Severity:** Impact of cyber events are constantly evolving.
- **Risk Type:** It is an inherent risk (i.e., WannaCry, Petya, notPetya) and not always targeted.
- **Risk Transfer** can alleviate some concerns, but solution has to extend beyond insurance.
- **Risk Engineering:** Investment in infrastructure and changes in culture can help mitigate exposures.

What is your tolerance for risk?

Thank you

The information in this publication was compiled from sources believed to be reliable for informational purposes only. All sample policies and procedures herein should serve as a guideline, which you can use to create your own policies and procedures. We trust that you will customize these samples to reflect your own operations and believe that these samples may serve as a helpful platform for this endeavor. Any and all information contained herein is not intended to constitute advice (particularly not legal advice). Accordingly, persons requiring advice should consult independent advisors when developing programs and policies. We do not guarantee the accuracy of this information or any results and further assume no liability in connection with this publication and sample policies and procedures, including any information, methods or safety suggestions contained herein. We undertake no obligation to publicly update or revise any of this information, whether to reflect new information, future developments, events or circumstances or otherwise. Moreover, Zurich reminds you that this cannot be assumed to contain every acceptable safety and compliance procedure or that additional procedures might not be appropriate under the circumstances. The subject matter of this publication is not tied to any specific insurance product nor will adopting these policies and procedures ensure coverage under any insurance policy.