AGC 2020 CONVENTION The Constr

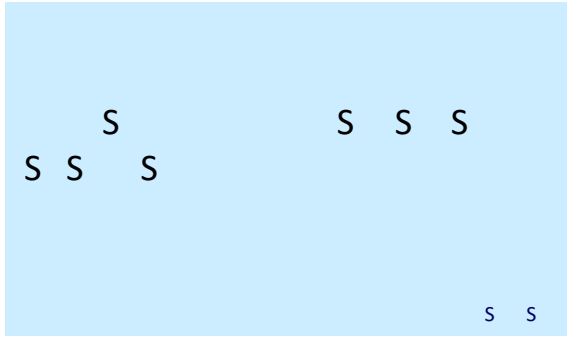
0.1 IACET CEU | The Associated General Contractors of America (AGC) has been accredited as an Accredited Provider by The International Association for Continuing Education and Training (IACET). In obtaining this accreditation, AGC has demonstrated that it complies with the ANSI/IACET Standard which is recognized internationally as a standard of

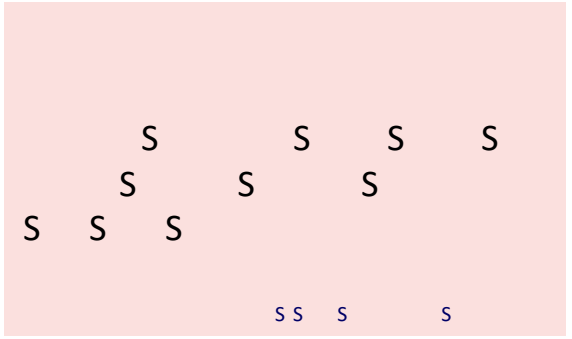
By the end of this session, participants will be able to:

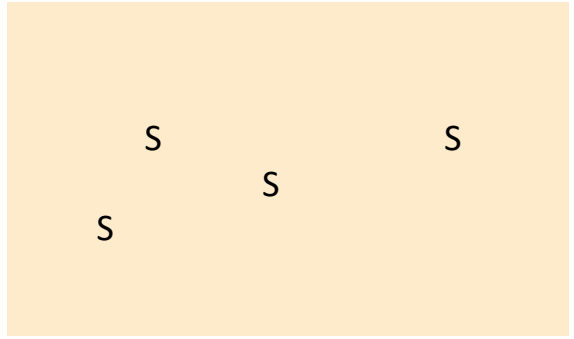
1. Examine cyber risk activity in the construction industry.
2. Identify the most common cyber security risks.
3. Discuss ways to help protect your organization from cyberattacks.
4. Explore how an information security management system (SMS) can help you develop effective and robust cyber security for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

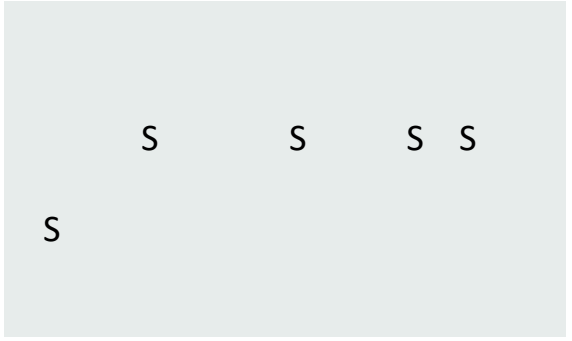
Terminology

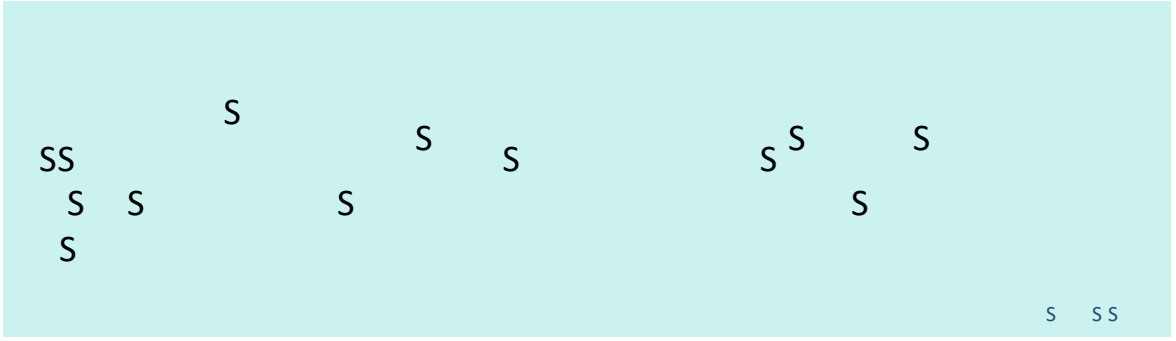
Cyber	Having to do with a computer or a computing system
IoT	“Internet of Things” relates to any device that can be connected to the internet.
Threat	Any circumstance or event with the potential to cause harm to an information system. Related terms: Threat actor = Bad guy Threat vector = Modus operandi

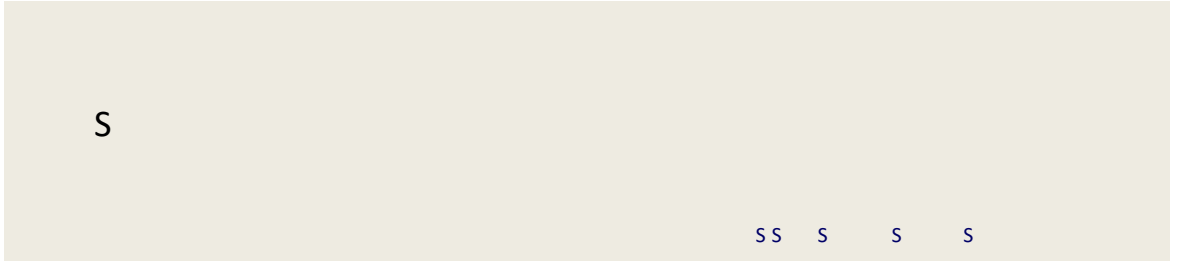


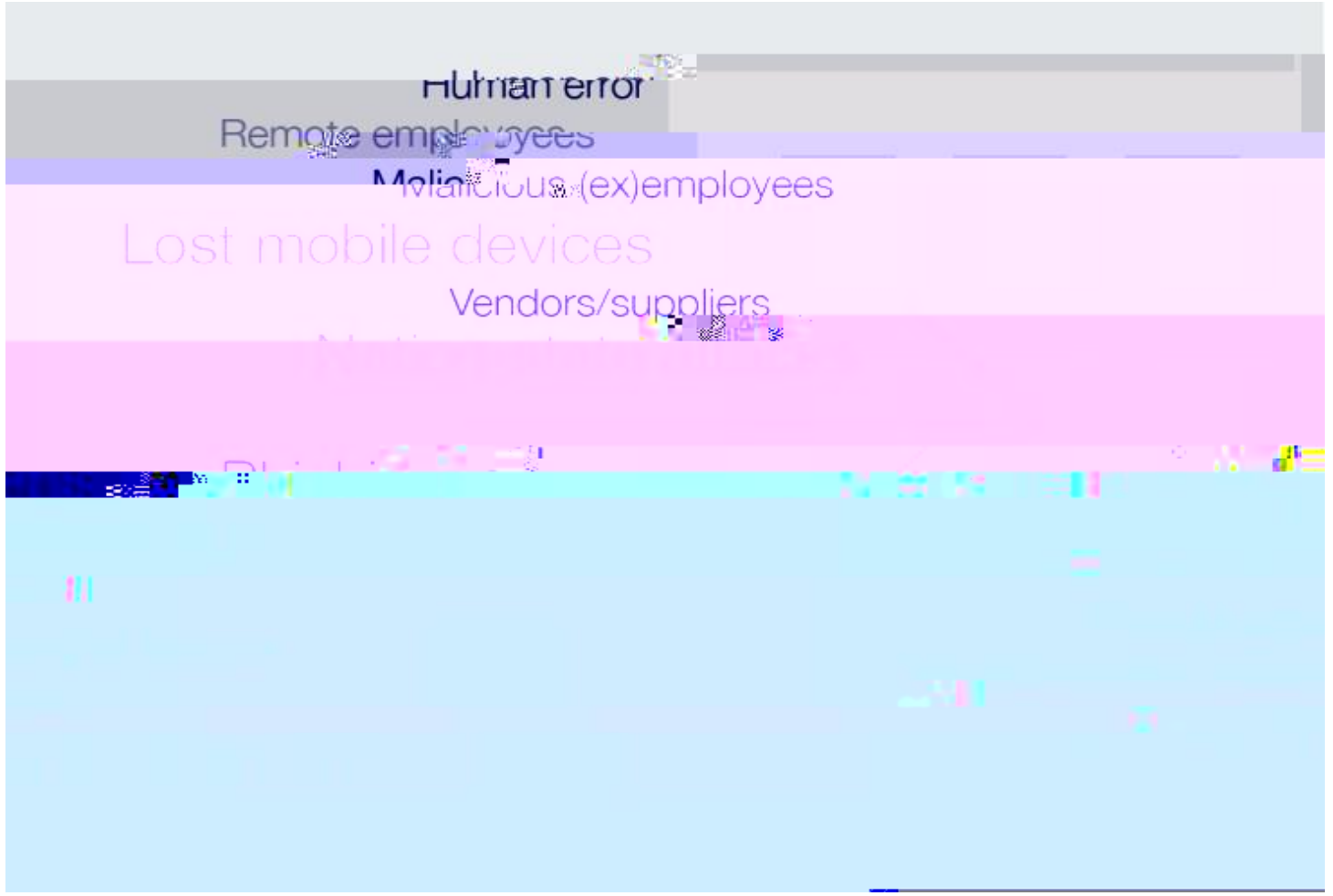


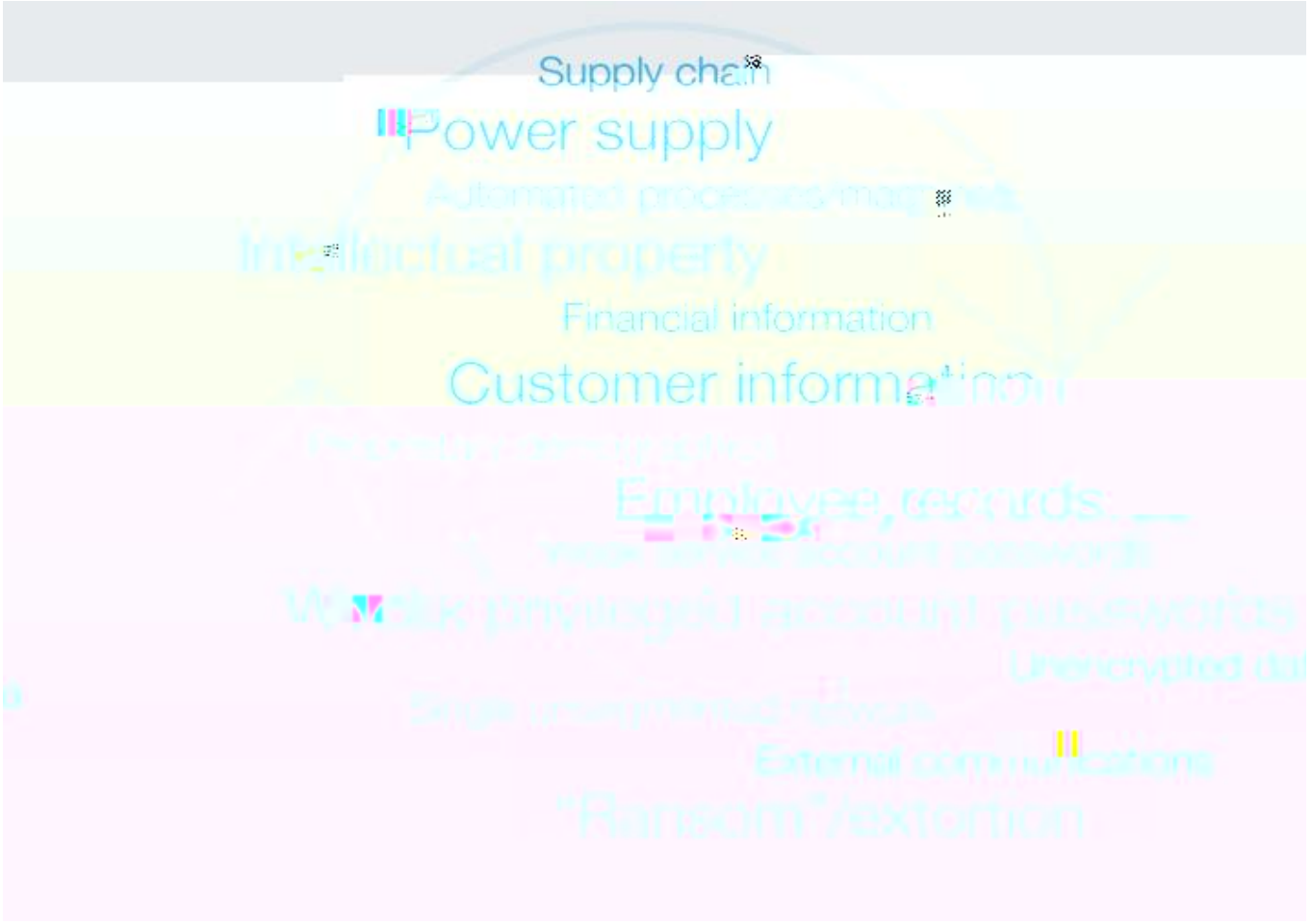




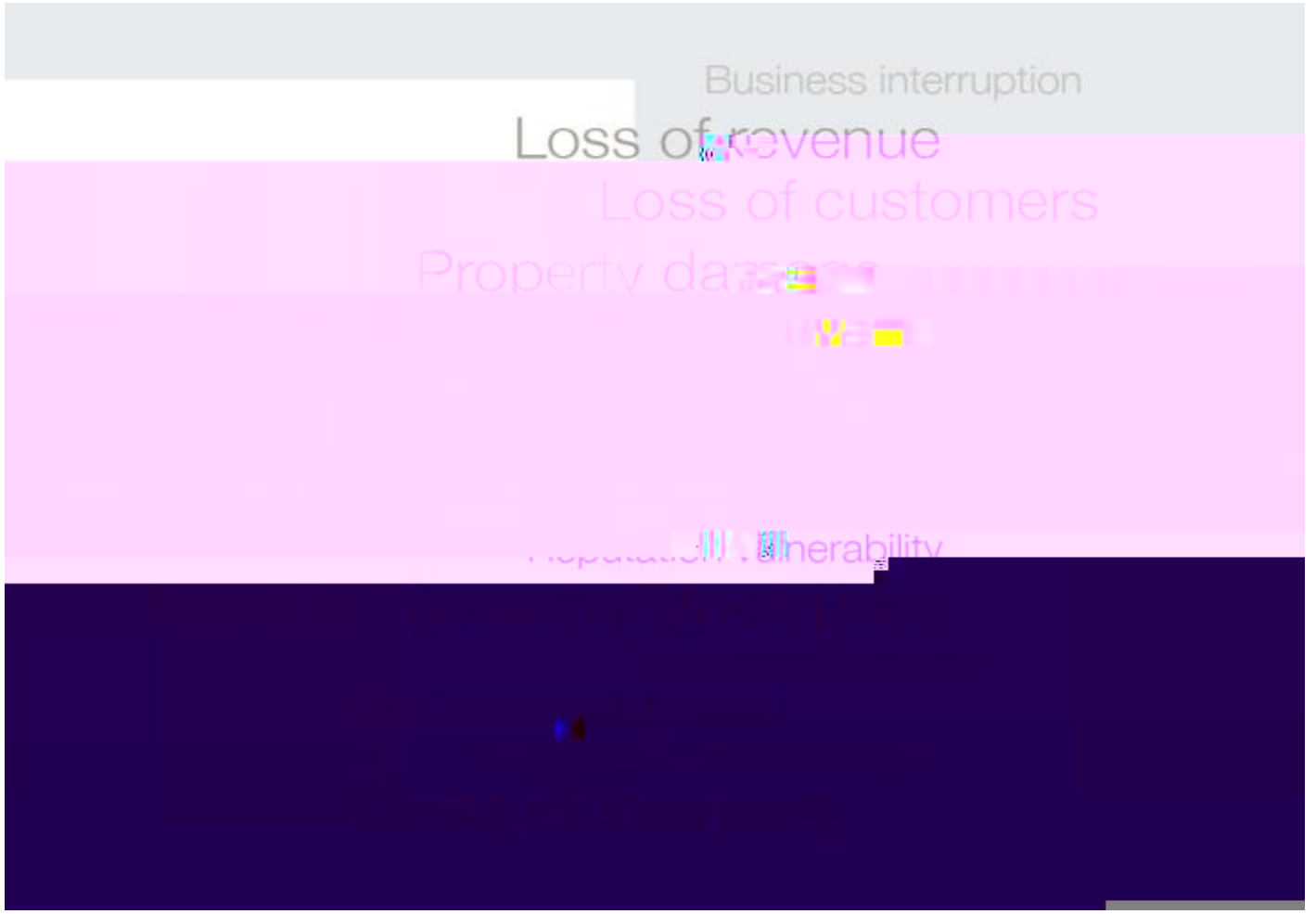





Human error
Remote employees
Malicious (ex)employees
Lost mobile devices
Vendors/suppliers


Supply chain
Power supply
Intellectual property
Financial information
Customer information
Employee records
External communications
"Ransom"/extortion

Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
Man-in-the-middle (MitM) attack
Phishing and spear phishing attacks
SQL injection attack
Drive-by Attack
Zero-Day attack
Malware
Ransomware
Wire Fraud
Cross-site scripting (XSS) attack
DNS Tunneling
Account Takeover
Trojans


Business interruption
Loss of revenue
Loss of customers

- 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

- 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?

The information in this publication was compiled from sources believed to be reliable for informational purposes only. All