

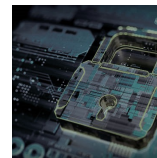


1



2

CYBER RISK – A LOOK BACK AT 2021



- Colonial Pipeline- \$4.4M paid to DarkSide (\$2.3M recovered by the Dept. of Justice)
- JBS USA - \$11M in cryptocurrency paid to Revil
- SolarWinds(Orion technology software)- more than 18,000 organizations impacted
- Microsoft Exchange Server/Microsoft Outlook Web Access (OWA) email systems vulnerabilities
- Kaseya- Impacted 800 to 1500 customers
- Log4j – currently being exploited

Risk Rewarded



3

CYBER RISK – PREDICTIONS FOR 2022



“Digital threats of all sorts are growing faster than the capability to defend against them. If past is prologue, 2022 is likely to be a year of big hacks, big threats and plenty more crises.”¹

2022 started with the log4j crisis. Per Jen Easterly, Director of CISA, *“the most serious vulnerability I have seen in my decades-long career.”*

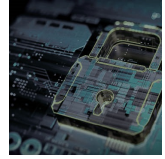
¹ 202 The Cybersecurity, Washington Post, Joseph Marks

Risk Rewarded



4

CURRENT CYBER RISKS



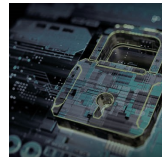
- **Social Engineering Fraud – phishing, baiting, spoofing and tailgating**
- **Fraudulent Wire Transfer Fraud**
- **Data Breaches due to third-party vendors**
- **Malware resulting in ransomware demands**
- **Distributed denial-of-service (DDoS) attacks**
- **Internet of Things (IoT)**
- **Ransomware-as-a-Service (RaaS)**

Risk Rewarded



5

CONSTRUCTION INDUSTRY CYBER RISKS



- **Level of cyber security and technology infrastructure**
- **Use of new technologies, artificial intelligence, IoT, drones**
- **Confidential and proprietary information collected, stored and shared with project owners and project participants (vendors, subcontractors, etc.)**
- **Reliance on supply chain**
- **Business Interruption**
- **Breach of Intellectual Property**

Risk Rewarded



6

HOW DO YOU PROTECT YOUR COMPANY FROM CYBER LOSS?

Risk Rewarded



7

RISK MANAGEMENT STRATEGIES



- **Avoid** – if a risk presents a potential negative consequence, you may choose to avoid those consequences by stepping away from the activities or carve-out the risks, thus avoiding the negative outcome.
- **Control**- identify the risk, minimize the potential for loss, implement processes to minimize the loss rather than eliminate it.
- **Retain**- acknowledge the possibility of certain risks and elect to accept the risk.
- **Transfer**- shift the burden of the risk consequence to another party in event something goes wrong. Insurance as an example.

Risk Rewarded



8

HELP-ful Suggestions



How –

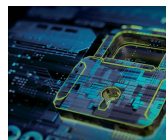
- Establish good cyber hygiene
 - Implement Multi Factor Authentication (MFA) across the entire network
 - Require strong passwords
 - Regularly backup your data and store separately
 - Ensure your software is up to date
 - Encrypt sensitive data and laptops
- Establish a culture of security, every employee will be your frontline of defense
- Educate yourself about current scams
- Evaluate your external network presence through Vulnerability Scans

Risk Rewarded



9

HELP-ful Suggestions



Establish-

- Dual controls for wire transfers
- Requirements that any changes to payment instructions are voice-verified at a pre-established number
- Processes to limit access to your computers and network components for those who need access
- Protocols to implement software patches as soon as possible
- Security requirements for all third-party vendors, subcontractors

Risk Rewarded



10

HELP-ful Suggestions



Leverage – resources available to you.

- Ask your bank to assist with audit and/or suggestions for changes to your wire transfer protocols
- Request your Auditing firm perform a cyber audit
- Utilize the free resources available through FTC, SBA, CISA
- If you purchase cyber insurance – utilize the free (or discounted) services offered to policyholders
- Utilize services offered by your insurance broker

Risk Rewarded



11

HELP-ful Suggestions



Plan-

- Create a cyber security plan that outlines the steps to be taken after a cyber event is discovered
- Assign key senior manager(s) responsible for the crisis management plan
- Identify internal team members
- Identify key outside vendors – legal counsel, forensics, IT resources, cyber insurance resources
- Develop your crisis management plan
- Test your crisis management plan through “table-top” simulation

Risk Rewarded



12

RESOURCES

- CYBERSECURITY AND INFRASTRUCTURE AGENCY (CISA) – THE BASICS FOR BUILDING A CULTURE OF CYBER READINESS [CYBER ESSENTIALS TOOLKITS | CISA](#)
- FEDERAL TRADE COMMISSION (FTC) [BUSINESS CENTER | FEDERAL TRADE COMMISSION \(FTC.GOV\)](#)
- INTERNET CRIME COMPLAINT CENTER (IC3) - [INTERNET CRIME COMPLAINT CENTER\(IC3\) | HOME PAGE](#)
- CSDZ – WWW.CSDZ.COM
- SHARON SCHARF - [SSCHARF@CSDZ.COM](mailto:sscharf@csdz.com)

Risk Rewarded

