Are You Extortion-Ready:
An Executive Guide To Successful Cyber Extortion Negotiation

An Expert Panel
Beazley, Coveware, Norton Rose Fulbright, FireEye
Today’s Panel

Kim Horn, Global Claims Leader, Cyber & Tech, Beazley

Bill Siegel, CEO & Founder, Coveware

Navid Jam, Managing Director, FireEye Mandiant

Steve Roosa, Partner, Norton Rose Fulbright
“Making ransomware unprofitable is effectively the only way, short of coordinated global regulation of cryptocurrencies, to stop these criminals”

— Josephine Wolff
Tufts Professor
Extortion Amounts are Rising – Especially for Large Enterprises

$36,295
+184%
Q2/Q1 2019

*Coveware 2019
Average Company Size

925 employees
up from 115
Q2/Q1 2019

Larger Companies are Being Targeted

Size of Victim Company by Number of Employees

*Coveware 2019
Demands for Certain Variants are Extremely High for Large Enterprises

Extortion Amounts

$1m + demands are now routine

Average Ransom Amount: Top 3 Ransomware Types

- Dharma: $13,925.1
- Ryuk: $267,742.5
- Sodinokibi: $56,577.8

*Coveware 2019
#1 Social Engineering

**Attack Vectors Change Monthly**

*Coveware 2019*
Cyber Extortion Discussion

- The role of the “breach coach”
- Insurance Considerations
- The role of Digital Forensics & Incident Response
- Working Groups & Communications
- Setting strategy along multiple paths of recovery
Cyber Extortion Discussion

- Threat Actor Communications
- Proof of Decryption
- Negotiation Strategy
- Crypto Currency Procurement
- Regulatory Considerations
- Financial Operations Preparedness
Cyber Extortion Discussion

- Preparing the network
- Speed vs Safety
- Prioritizing restoration of services
- Common misconceptions and pitfalls
Questions?