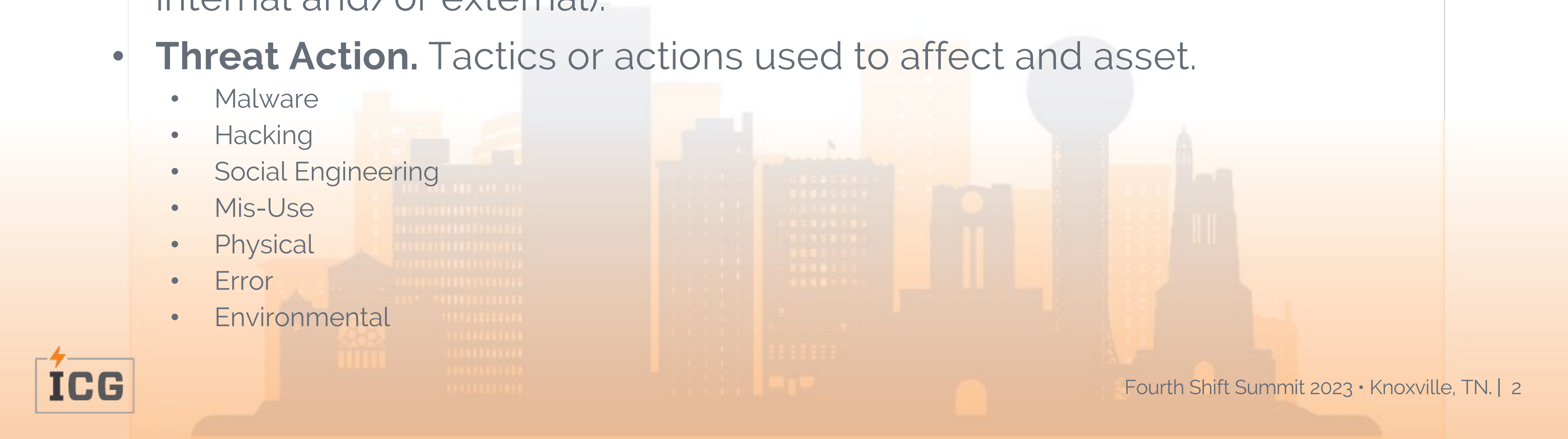
CYBER SECURITY IN MANUFACTURING AND ICG\DATAGUARD365

JERRY HOOK, CTO

CYBERSECURITY TERMINOLOGY

- **Incident.** A security event that compromises the integrity or availability of information.
- **Breach.** An incident that results in the confirmed disclosure of data to an unauthorized party.
- **Threat Actor.** A person or persons behind a security event (can be internal and/or external).
- **Threat Action.** Tactics or actions used to affect and asset.
  - Malware
  - Hacking
  - Social Engineering
  - Mis-Use
  - Physical
  - Error
  - Environmental



SUMMARY OF

BREACHES AND INCIDENTS

- 74% of all breaches include a human element via air, privilege misuse, stolen credentials or social engineering.
- 83% of all breaches involve external threat actors.
- 95% of all breaches were financially driven.
- 3 primary ways in which attackers access an organization includes:
  - Stolen Credentials
  - Phishing
  - Exploitation of Vulnerabilities
- 24% of all breaches involved ransomware. (Continues to hold the top spot.)
- 49% of all breaches involved credentials.

RESULTS AND ANALYSIS

BREACHES AND INCIDENTS

Percentage of Breaches and Incidents:

- 83% due to External Threat Actors.
  - 70% are from Organized Crime.
- 19 % due to internal.
- 94.6% are financially driven.

Resultant Actions:

- 40% Stolen Credit Cards
- 24% Ransomware
- 15% Phishing

Areas of Breaches:

- 60% Web Apps
- 30% Mail Servers

INCIDENT CLASSIFICATION PATTERNS

System Intrusion	Social Engineering	Web App Attacks	Denial of Service	Lost and Stolen Assets	Privilege Misuse
• 3,966 Incidents with 1944 with confirmed data disclosure. • 96% were external threat actors. • 97% was financially driven. • 42% Other, 34% Personal, 31% System • Top most common ways in: Email, desktop sharing software, web apps.	• 1700 incidents with 928 confirmed data disclosures • 100% were external threat actors • 89% financially driven • 11% espionage • stolen credentials 76% • 28% internal • personal 26%	• 1404 incidents, 1315 data disclosure • 100% external • 95% financial • 86% data compromised credentials • 72% personal	• 6248 incidents, 4 compromised data. • Top spot and has been for years of incidents.	• 2091 incidents, 159 data disclosure • 92% external • 68% internal • 100% financial • 87% personal data • 30% medical • 13% banking	• 406 incidents, 288 data disclosure • 99% internal • 89% financial • 13% grudge • 5% espionage • 73% data compromised • 73% personal • 34% medical

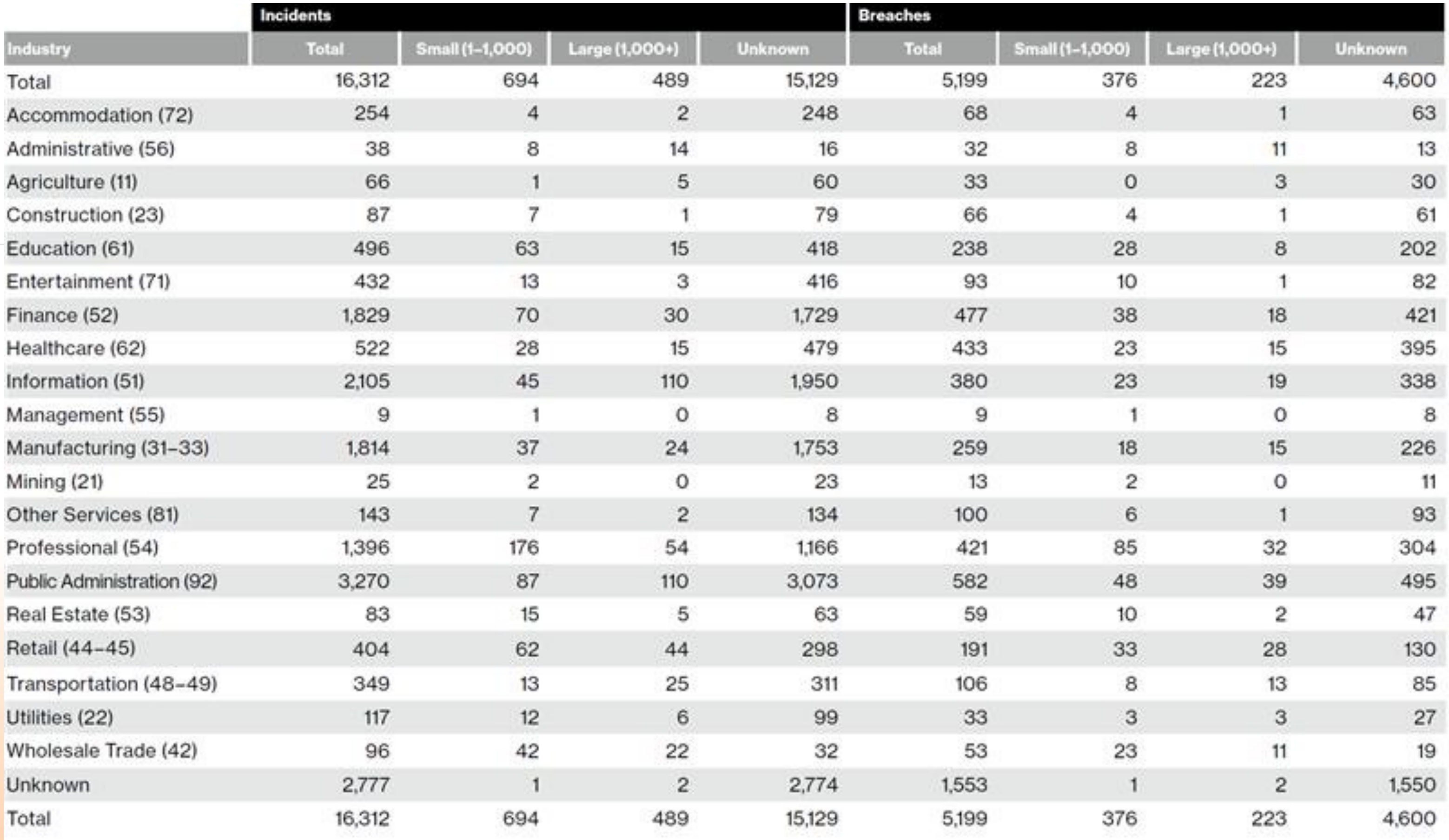
INCIDENT CLASSIFICATION PATTERNS

ICG

System Intrusion	Social Engineering	Web App Attacks	Denial of Service	Lost and Stolen Assets	Privilege Misuse
• 3,966 Incidents with 1944 with confirmed data disclosure. • 96% were external threat actors. • 97% was financially driven. • 42% Other, 34% apps.	• 1700 incidents with 928 confirmed data disclosures • 100% were external threat actors • 89% financially driven • 11% espionage	• 1404 incidents, 1315 data disclosure • 100% external • 95% financial • 86% data compromised credentials • 72% personal	• 6248 incidents, 4 compromised data. • Top spot and has been for years of incidents.	• 2091 incidents, 159 data disclosure • 92% external • 68% internal • 100% financial • 87% personal data • 30% medical • 13% banking	• 406 incidents, 288 data disclosure • 99% internal • 89% financial • 13% grudge • 5% espionage • 73% data compromised • 73% personal

This pattern, which accounts for 25% of our breaches, consists largely of leveraging stolen credentials and vulnerabilities to get access to an organizations' assets. With this beachhead, the attackers can then do a variety of things, such as stealing key information hiding in emails or asking code from repositories. While these attacks aren't complicated, they certainly are effective and have remained a relatively stable part of our dataset, which prompts us to discuss once again (drum roll, please), the importance of multifactor authentication MFA) and patch management!

INDUSTRIES INTRODUCTION



	Incidents				Breaches			
Industry	Total	Small (1–1,000)	Large (1,000+)	Unknown	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	16,312	694	489	15,129	5,199	376	223	4,600
Accommodation (72)	254	4	2	248	68	4	1	63
Administrative (56)	38	8	14	16	32	8	11	13
Agriculture (11)	66	1	5	60	33	0	3	30
Construction (23)	87	7	1	79	66	4	1	61
Education (61)	496	63	15	418	238	28	8	202
Entertainment (71)	432	13	3	416	93	10	1	82
Finance (52)	1,829	70	30	1,729	477	38	18	421
Healthcare (62)	522	28	15	479	433	23	15	395
Information (51)	2,105	45	110	1,950	380	23	19	338
Management (55)	9	1	0	8	9	1	0	8
Manufacturing (31–33)	1,814	37	24	1,753	259	18	15	226
Mining (21)	25	2	0	23	13	2	0	11
Other Services (81)	143	7	2	134	100	6	1	93
Professional (54)	1,396	176	54	1,166	421	85	32	304
Public Administration (92)	3,270	87	110	3,073	582	48	39	495
Real Estate (53)	83	15	5	63	59	10	2	47
Retail (44–45)	404	62	44	298	191	33	28	130
Transportation (48–49)	349	13	25	311	106	8	13	85
Utilities (22)	117	12	6	99	33	3	3	27
Wholesale Trade (42)	96	42	22	32	53	23	11	19
Unknown	2,777	1	2	2,774	1,553	1	2	1,550
Total	16,312	694	489	15,129	5,199	376	223	4,600

INDUSTRIES - MANUFACTURING FOCUSED

- 1817 incidents, 262 confirmed data disclosure.
- Patterns:
  - System Intrusion
  - Social Engineering
  - Web App Attacks (83% of all breaches)
- 90% External Threat Actors.
- 86% Financial Motives.
- Data Compromised:
  - 60% Personal
  - 68% Credentials

HOW CAN WE PREVENT THIS?

ICG\DATAGUARD 365

CYBERSECURITY WITHOUT THE COMPLEXITY

- Our industry is led to believe the more you spend on cybersecurity, the more secure you will be.
- Research shows that companies that spend the most on cybersecurity programs falls short compared to the rest of the industry.
- Detect, protect and respond against cyberattacks in real time.
  - Simple, Proactive, and Fast.

SIMPLE
Get the IT security you need without any complications or any unnecessary expense

PROACTIVE
Anticipate cyber attacks before they harm your environment

FAST
Tackle security breaches faster than the industry average

ICG\DATAGUARD 365

CYBERSECURITY WITHOUT THE COMPLEXITY

Managed Detection and Response (MDR)

Achieve greater visibility and real-time response capabilities using Artificial Intelligence (AI) and advanced cybersecurity tools designed to deliver a comprehensive protection against cyber threats.

Incident Response Retainer (IRR)

We'll help you create a clear, thorough, and structured approach to identifying, containing, investigating, and resolving a security incident or data breach.

24/7 Security Operations Center (SOC)

As an extension of your team, our expert analysts actively monitor, triage, prioritize, and respond 24/7 to ensure a no-breach, a no-loss, business-as-usual experience.

EVEN MORE FEATURES

Managed Security Awareness
Penetration Testing
Zero-Trust Framework
CISO Collaboration
Data Loss Prevention

METRICS REPORTING

> 4 min Avg Incident Response

SAMPLE SOC FEATURES

Digital Forensics
Incident Response
Continuous Monitoring
Advanced Threat Detection
Expert Security Analysis
Real-Time Alert and Notification
Detailed Client Support
Threat Hunting

ICG\DATAGUARD 365

TECHNOLOGY STACK

Quoted per
endpoint per month

SentinelOne Complete License

Quoted per
endpoint per month

SentinelOne Complete with 24/7 SOC & Incident Response

Quoted per
user per month

KnowBe4 | Fully Managed Security Awareness Program

Quoted to
specific needs and environment

Compliance Services

Quoted per
GB of avg daily usage

Stellar Cyber Next Gen SIEM

ICG\DATAGUARD 365

TECHNOLOGY STACK

Quoted per
endpoint per month

SentinelOne Complete License

Quoted per
endpoint per month

SentinelOne Complete with 24/7 SOC & Incident Response

Quoted per
user per month

KnowBe4 | Fully Managed Security Awareness Program

Quoted to
specific needs and environment

Compliance Services

Quoted per
GB of avg daily usage

Stellar Cyber Next Gen SIEM

SOC FEATURES

- Technical support by phone, web, and email
- In-product resource center / Support portal access
- Enterprise Support 24x7, Follow-the-Sun for Sev 1 & 2
- Designated Technical Account Manager + Enterprise Support
- Managed Detection & Response (MDR) Subscription
- Readiness Deployment & Ongoing Health Subscription
- Environment-Based Security Recommendations
- Potentially Malicious files tested in the Sandbox, as part of Threat Analysis
- Alert monitoring and Incident Response 24x7

SENTINELONE XDR FEATURES

- Autonomous Storyline engine
- Static AI & Cloud file-based attack prevention
- Behavioral AI fileless attack detection
- Autonomous Threat Response / Kill, Quarantine (Win, Mac, Linux)
- Autonomous Remediation Response / 1-Click, no scripting (Win, Mac)
- Autonomous Rollback Response / 1-Click, no scripting (Win)
- Quarantine devices from the network
- Incident Analysis (MITRE ATT&CK, timeline, explorer, team annotations)
- Agent anti-tamper
- App Inventory

Thank You!