Mantix4™

THE NEW DIMENSION IN CYBER INTELLIGENCE™

Business MANAGER 365™

20 Winning TECHNOLOGIES

CELEBRATING 20 YEARS

A Veteran Woman Owned Business

CJF COWELL | JAMES | FORGE

INSURANCE GROUP™

CYBERHUNTER

Mantix4™
THE NEW DIMENSION IN CYBER INTELLIGENCE™

Agenda

- Welcome and Introductions
- Terms
- Opening/Framing
- Case Study
  - Review Actual Breech/Ransom Attack
    - Anatomy of the Cyber Attack
    - How Reflects Cyber Threat Trends
    - Impact on Business (Highlight Risks)
  - How Could the Business Leader Have Proactively Prevented / Mitigated
    - Auditing and Vulnerability Testing
    - Integrated Solution: Managed Protection, Detection and Response, and Resiliency that supports Recovery
    - Cyber Insurance as Critical Part of Resiliency
- Q&A
- Closing Comments

Agenda

CJF COWELL | JAMES | FORGE INSURANCE GROUP™

CYBERHUNTER

20 Winning TECHNOLOGIES CELEBRATING 20 YEARS

Introductions

Christopher D. “Chuck” Taylor, Colonel USMC (Ret.)
Vice President of Sales, Mantix4 LLC

Chuck Taylor also serves as Vice President of Sales, Mantix4 LLC and Chief Executive Officer, Sales Sortie, LLC. He has previously served as President and founder of a consulting firm providing leadership and training consulting to governments and private sector businesses globally. Chuck has also served globally with an elite former Military team providing leadership, performance, and risk management coaching to industry executives, high-level staffs, and operators in the field conducting high consequence operations.

Scott Lewis
President and CEO of Winning Technologies Group of Companies, including Liberty One Software.

Scott has more than 41 years of experience in the technology industry, managing systems as small as a few users and as large as thousands of users. Scott is a nationally recognized speaker and author on technology subjects. Scott has worked with hundreds of large and small businesses to empower them to use technology to improve work processes, increase productivity, and reduce costs. Scott has designed thousands of systems for large, medium, and small companies. Winning Technologies' goal is to work with companies to select, implement, manage, and support technology resources.

Chris Dodunski
Chief Executive Officer, CyberHunter Solutions & Chief Technology Officer, Mantix4 LLC

Chris Dodunski is an entrepreneurial, hands-on engineer with over 30 years of experience identifying and implementing technologies and enterprise systems that achieve key business objectives. He brings broad expertise in IT, data networking, cyber security, telecommunications architecture/infrastructure design, full project life cycle management, and client/vendor relationship management.

Deena James
CEO & COO of Cowell James Forge Insurance | Service Above Self | Proud Grandmother | Woman of Faith | Chiefs Fanatic

I began my insurance career right out of high school as a way to pay for college. I worked my way from the file room to the CEO of the Krueger & James Agency and now as the CEO of Cowell James Forge Insurance Agency, learning along the way all the intricacies of insurance and how to manage risk for customers. I'm just crazy enough to love to read those insurance policies that most everyone files quickly away! I've stayed in the business for over 40 years because I love knowing that I can make a difference in an awful situation by having the proper insurance in place.

Mantix4™ THE NEW DIMENSION IN CYBER INTELLIGENCE™

CYBERHUNTER

CJF COWELL | JAMES | FORGE INSURANCE GROUP ™

20 Winning TECHNOLOGIES CELEBRATING 20 YEARS

Cybersecurity Terms

- **Cyber Security** -- Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.
- **Breech** -- A data breach is a security violation, in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, altered or used by an individual unauthorized to do so.
- **Ransom Attack** -- Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off.
- **Upstream Damage** -- In computer networking, upstream refers to the direction in which data can be transferred from the client to the server.
- **Downstream Damage** -- One process sending data primarily in the **downstream** direction is downloading.
- **End-Points** -- An **endpoint** is a remote computing device that communicates back and forth with a **network** to which it is connected. Examples of **endpoints** include Desktops Laptops Smartphones Tablets Servers Workstations Internet-**of**-things (IoT) devices **Endpoints** represent key vulnerable **points of** entry for cybercriminals.
- **Vulnerabilities** -- A **network vulnerability is** a flaw or weakness in your IT processes that could allow someone to gain access, steal data, or otherwise cause you harm.
- **Assets** --In information security, computer security and network security, an asset is any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware, software and confidential information.
- **Incident Response** -- **Incident response** (sometimes called cybersecurity **incident response**) refers to an organization's processes and technologies for detecting and responding to cyberthreats, security breaches or cyberattacks.
- **Types of Attacks** – Malware, Denial of Service, Phishing, Spoofing, Identity based attacks, Code injection, Supply Chain, Insider threat, DNS Tunneling, Internet of things
- **Threat Vectors** -- A **threat vector is** a path or a means by which a cybercriminal gains access through one or more of six main routes into a computer system by exploiting a route vulnerability (also called an attack surface).
- **EDR** -- Endpoint Detection and Response (**EDR**), also referred to as endpoint detection and threat response (EDTR), is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.
- **XDR** -- Extended detection and response (**XDR**) defined Extended detection and response, often abbreviated (**XDR**), **is** a software as a service (SaaS) tool that offers holistic, optimized security by integrating security products and data into simplified solutions.
- **Penetration Testing** -- **Penetration testing** (or pen **testing**) **is** a security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a computer system. The purpose of this simulated attack is to identify any weak spots in a system's defenses which attackers could take advantage **of.**
- **Security Based Technology Audit** -- A **security audit is** a systematic evaluation of the **security of** a company's information system by measuring how well it conforms to an established set of criteria. A thorough **audit** typically assesses the **security of the** system's physical configuration and environment, software, information handling processes and user practices.

Case Study – The Breech

- Company – Texas based
- Size – National
- Industry – General Contractor
- Attack – Man in Middle -- Phishing
- Date of Attack – later part of 2019
- Attacker captured emails between Finance Department and Bank
- The bank and victim knew each other – use to trading emails and processing payments
- Using O365
- Original email looked ligament
- Used Human conditioning, and social engineering to fool bank into a transfer
- Transferred $480,000.00 Dollars
- Recovery = 0.00

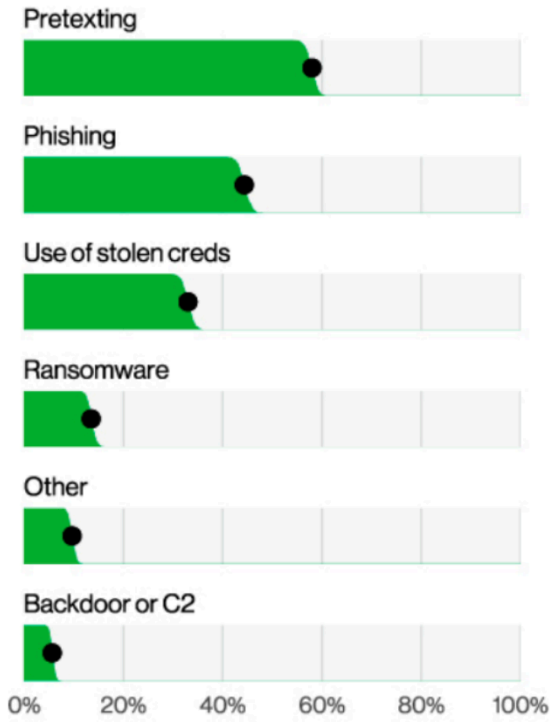
The insurer denied the claim because they said it did not cover CEO fraud or business email compromise as a result of spear phishing. According to the policy, it would only cover the cyber event if it involved a forgery of a financial instrument.

Case Study – Areas of Improvement

- Educate Users – Continuously Educate and Test user community
- Upgrade hardware and software don't keep either past useful lifecycle -- Get rid of old hardware and keep software current.
- Audit Systems Regularly --- Security IT Auditing at least annually
- Implement XDR/EDR Solutions – Mantix4
- Multi-Factor Solutions all users that access any part of your system
- Technology Integration --- Mantix4, Cisco, Sentinel One, Business Manager 365, DUO as examples
- Separation of Duties – Have an outside party looking over the security of your systems
- Policies and Processes to verify financial transactions.
- Proactive Patch Management
- Proactive Monitoring of systems and security
- Penetration Testing

Social Engineering Statistics - 2023

Top Method of Initial Entry



- Pretexting attacks are where a threat actor pretends to be a known entity and uses emotion and social engineering techniques to get the victim to do something they want.
- One of the more complex social attacks is the BEC. In these pretexting attacks, actors leverage existing email threads and context to request that the recipient conduct a relatively routine task, such as updating a vendor's bank account. However, the new bank account belongs to the attacker.
- Pretexting is now more prevalent than Phishing in Social Engineering incidents. However, when we look at confirmed breaches, Phishing is still on top.

Cyber Threat Highlights - 2023

- 74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering
- 83% of breaches involved External actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 95% of breaches.
- The three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities.
- Business Email Compromise (BEC) attacks have almost doubled across the entire 2023 incident dataset (approx 953,000 reported incidents), and now represent more than 50% of incidents within the Social Engineering pattern.
- Ransomware continues its reign as one of the top Action types present in breaches, and while it did not actually grow in 2023, it did hold statistically steady at 24%
- Other areas of increasing concern: Denial of Service (top category for incidents, not breaches), Lost & Stolen Assets (phones, laptops).

ISACA

CISA
CERTIFIED INFORMATION SYSTEMS AUDITOR

CISM
CERTIFIED INFORMATION SECURITY MANAGER

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Auditing and Strategic Planning

Components of a ISACA / CoBit Security Based IT Audit Building IT Strategy on a Framework for Success.

- Infrastructure Security Evaluation
- Server Security and Evaluation
- Digital Storage
- Security Awareness Training
- EDR/XDR Evaluation
- Electronic Mail Security Evaluation
- Policy and Procedures
- Disaster Recovery
- Business Continuation
- Asset Identification – Hardware, Software, Other
- Software Licensing Compliancy
- Firewall and Intrusion Detection
- Patch Management
- System Monitoring
- Physical System Security Evaluation
- Backup and Restoration Evaluation

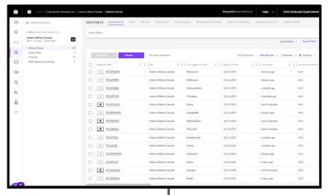
Mantix4™ THE NEW DIMENSION IN CYBER INTELLIGENCE™

CYBERHUNTER

CJF COWELL | JAMES | FORGE INSURANCE GROUP™

20 Winning TECHNOLOGIES CELEBRATING 20 YEARS

UX Portals



Mantix4
THE NEW DIMENSION IN CYBER INTELLIGENCE

Cloud Threat Detection
(Assets & Services)

Endpoint Activity Monitoring

Network Traffic Analysis

EDR / XDR Observations

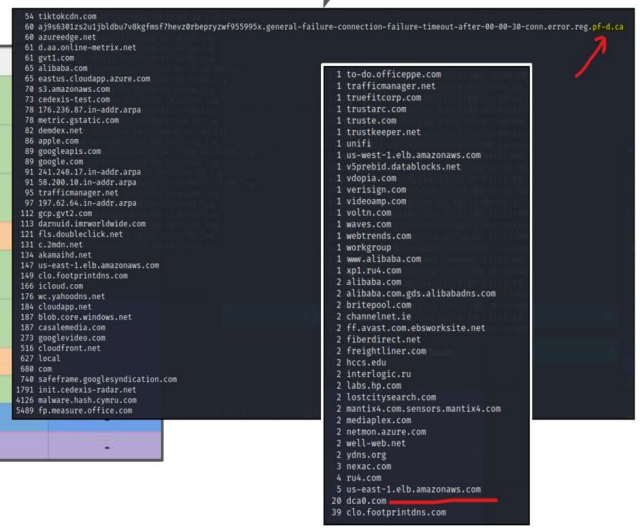
Threat Hunting

+

Per Host ML, Risk & Analytics OD

Common Message Bus / API

Timestamp	System	MITRE Tech	Mitre Tactic	Description
Sep 26, 2022 @ 20:44:15.298	PC2C1V52	T1053	Execution, Persistence, Privilege Escalation	Sysmon - Event 7: Image loaded by C:\\Windows\\System32\\taskhostw.exe
Sep 26, 2022 @ 20:44:28.698	PC2C1V52	T1016	Discovery	MITRE T1016 System Network Configuration Discovery: C:\\Windows\\SysWOW64\\ipconfig.exe
Sep 26, 2022 @ 20:44:31.102	PC2C1V52	T1016	Discovery	MITRE T1016 System Network Configuration Discovery: C:\\Windows\\SysWOW64\\ipconfig.exe
Sep 26, 2022 @ 20:44:37.196	PC2C1V52	T1071	Command and Control	DNS Stats - Low Frequency Score in Queried Domain
Sep 26, 2022 @ 20:47:41.048	PC2C1V52	T1016	Discovery	MITRE T1016 System Network Configuration Discovery: C:\\Windows\\SysWOW64\\ipconfig.exe
Sep 26, 2022 @ 20:47:42.853	PC2C1V52	T1016	Discovery	MITRE T1016 System Network Configuration Discovery: C:\\Windows\\SysWOW64\\ipconfig.exe
Sep 26, 2022 @ 20:47:49.870	PC2C1V52	T1071	Command and Control	DNS Stats - Low Frequency Score in Queried Domain
Sep 26, 2022 @ 20:49:30.787	PC2C1V52	T1204	Execution	Sysmon - Event 1: Process creation Windows Command Processor
Sep 26, 2022 @ 20:49:58.908	PC2C1V52	T1059	Execution	**MITRE T1059 Command-Line Interface: D:\\Release\\Akagi64.exe**
Sep 26, 2022 @ 21:46:10.792	PC2C1V52	T1204	Execution	**SentinelOne - New Suspicious threat detected - machine PC2C1V52**



NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

ISACA

Review, Document, Modify Security Plan

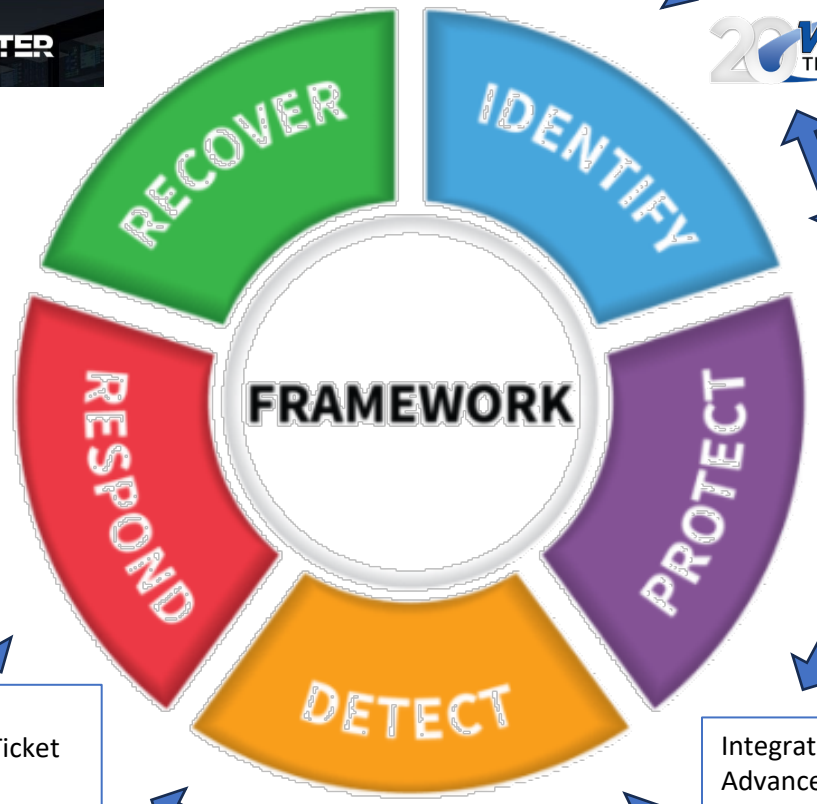
Remediation process and recovery process

CYBERHUNTER

Winning TECHNOLOGIES CELEBRATING 20 YEARS

Security Technology Audit – You must know what you're trying to protect, Hardware, Software, Applications, Data, and what your threat landscape looks like.

If deeper remediation processes or actual breech ticket will be escalated



Development of IT Strategic Plan

Create a Security Strategic Plan, based on accepted Security Framework, ISACA, CoBit, NIST or ISO

Business MANAGER 365

Mantix4 THE NEW DIMENSION IN CYBER INTELLIGENCE

Implementation of Security Based IT Strategy and Monitoring

Winning TECHNOLOGIES CELEBRATING 20 YEARS

Security Operations Center 24x7x365

Automated Alert Notification and Ticket Creation

Integration of Advanced Threat Protection, Firewalls, and MFA

Identify Threats, track, neutralize and quarantine known and unknown threats before they affect business operations

SentinelOne

Mantix4 THE NEW DIMENSION IN CYBER INTELLIGENCE

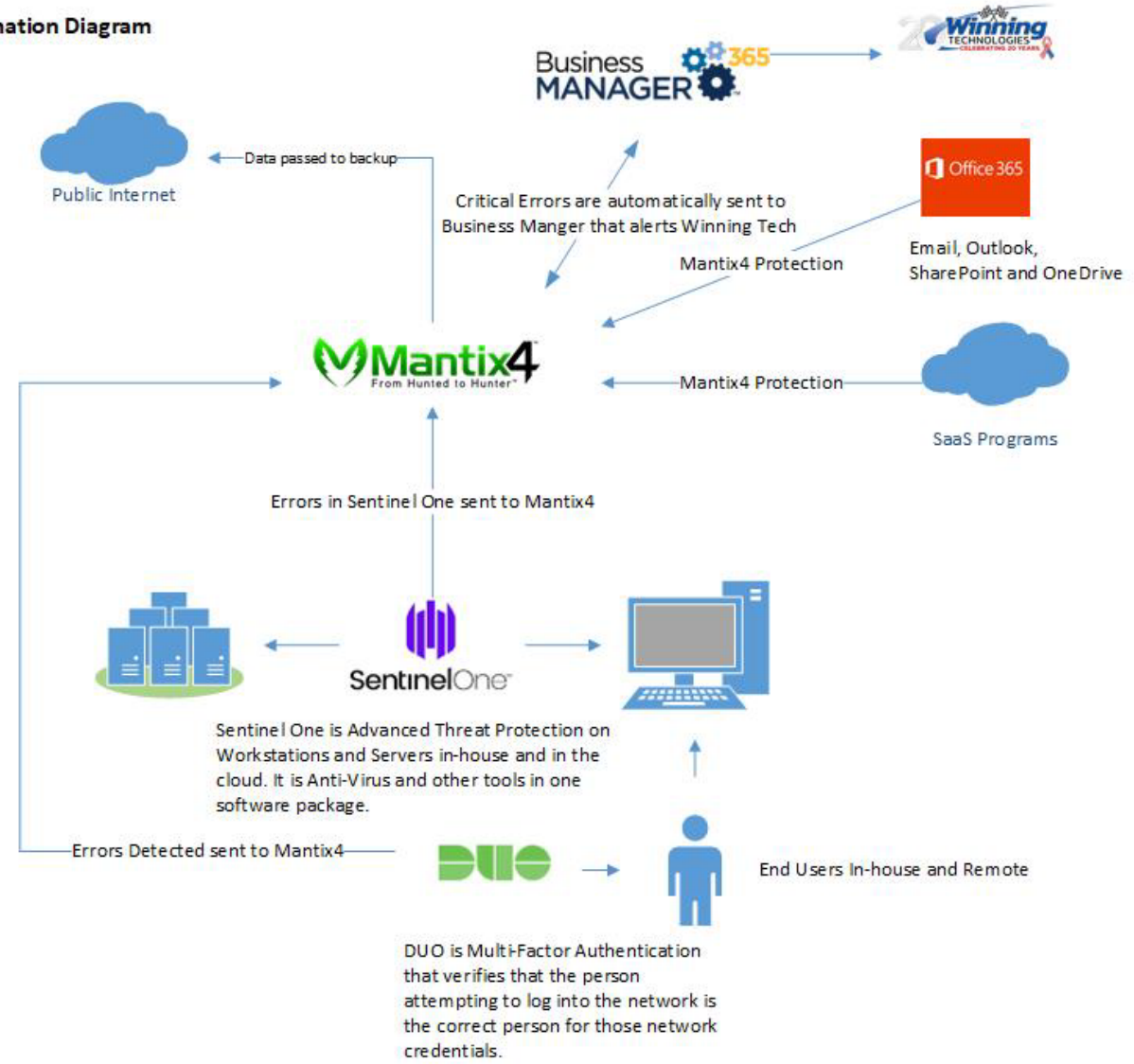
Mantix4 THE NEW DIMENSION IN CYBER INTELLIGENCE

Framework Integration for Total Security Management

Winning TECHNOLOGIES CELEBRATING 20 YEARS

Security Integration Modeling

Security Automation Diagram



Cyber Insurance

1. Do we have a cyber insurance policy?
2. Who owns the task of mitigating cyber risk with insurance?
3. Do we have the right amount of cyber insurance?
4. What does our policy cover?
5. Does our insurance provider understand our industry and its risks?
6. Is our policy flexible enough to adapt as our business grows?

Mantix4
THE NEW DIMENSION IN CYBER INTELLIGENCE

Question and Answers and any Follow-up

Business MANAGER 365

CYBERHUNTER

CJF COWELL | JAMES | FORGE INSURANCE GROUP ™

20 Winning TECHNOLOGIES CELEBRATING 20 YEARS

Ready to Purchase Mantix4, CyberHunter or Q-Net

Call Winning Technologies

877-379-8279 or Email sales@winningtech.com

Mantix4™
THE NEW DIMENSION IN CYBER INTELLIGENCE™

Business MANAGER 365™

20 Winning TECHNOLOGIES
CELEBRATING 20 YEARS

A Veteran Woman Owned Business

CJF COWELL | JAMES | FORGE
INSURANCE GROUP™

CYBERHUNTER