KROLL

Mid-Atlantic CIO Forum

The Ever-Changing Cybersecurity Battlefield

A CISO’s Proactive Approach Toward Cyber Risk Management

March 16, 2023

Table of Contents

Introductions

Ira Levy

Associate Managing Director, Washington DC

Qualification

MBA and MS in Information and Telecommunications from Johns Hopkins University

MA in Education from University of Central Florida

BA in Psychology from University of West Florida

Certified Information Security Professional (CISSP)

Doctoral candidate at The University of Maryland's School of Public Policy

Background & Relevant Experience

Ira Levy is an associate managing director in the Cyber Risk practice, based in Washington D.C. He leverages more than 20 years of experience in the both the public and private information technology sector, working within telecommunications, software development and managed services.

Prior to joining Kroll, Ira served as the executive director of the administrative modernization program at the University of Maryland. Before that, he held the title of chief operating officer at Affiniti, a national telecommunications and managed services company. Additionally, he previously served as CEO of Torrential Systems and chief information officer at Howard County Government in Maryland.

Ira's notable achievements include bringing five technology products to market including a network security solution adopted by a multitude of healthcare facilities and later acquired by national managed services company. Additionally, Ira lead the deployment of the One Maryland Inter-County Broadband Network (ICBN), which received a $115 million federal grant and was acknowledged by the White House for innovation and impact. Ira has also participated in numerous associations and boards, including the University of Maryland's Presidential 5G/6G Advisory committee, Broadband Council board, NACO, NATOA's CIO Advisory Council, the Howard County Tech Council, Digital Governing Communities, past Chair of Regional Fiber deployment committee, the Howard County Public School System Technology Vision committee, founding board member of the Howard County Tech Council and the Howard Community College Commission for the Future.

Further, Ira was recognized in the Daily Record's 40 under 40 and was named the HTC Technology Advocate of the Year, as well as the Public-Sector CIO of the Year by The Tech Council of Maryland. Ira was later named Smart CIO by SmartCEO magazine for his efforts addressing regional problems with innovative solutions and forging new partnerships to achieve significant cost savings.

John deCraen

Associate Managing Director, Dallas

Qualification

Twenty-five years experience

Numerous Industry Certifications

Computer Science Studies

Background

John is an Associate Managing Director in the Cyber Risk practice of Kroll, based in the Dallas office. He has over two decades of experience working with Global Fortune 500 businesses and AmLaw 100 law firms, delivering high-profile enterprise-class solutions enhanced with strategic and technical cyber security program leadership and guidance. He specializes in digital forensics, incident response, information security risk and compliance assessment matters that demand investigative and analytical thinking.

Prior to joining Kroll, John was a Senior Director with Alvarez & Marsal's Global Cyber Risk Services practice in Dallas. He was the original member of the firm's Global Cyber Risk Services practice, where he was heavily involved in developing the culture, systems design, standard procedures and talent management throughout its 16-year history. He was also the lead architect and implementor of the firm's data centers, systems and processes responsible for managing all the litigation support efforts for the world's two largest bankruptcies, simultaneously. These systems ultimately processed more than five petabytes of data and hosted data for more than 700 high-profile legal cases.

Previously, John has also led and substantially contributed to many digital forensics and cyber security investigations worldwide, which includes representing a state insurance commissioner and a U.S. regulatory body on a comprehensive and global examination of the world's largest insurance company's cyber security and privacy programs. Further, he also designed and built a real-time end-point vulnerability and risk scoring system for a leading national ONG pipeline management company.

John also has extensive experience in the strategy and architecture of complex computing environments that include infrastructure design, entitlement programs, policy development, standards implementation and risk management frameworks. He is particularly strong in the area of cyber risk assessment having assisted multiple clients in determining their alignment with NY-DFS, HIPAA/HiTrust, DFARS, GDPR, FFIEC, and a range of maturity and risk models. He also has expertise in one-on-one and panel-on-one interview and evidence collection.

Relevant Experience

John worked with clients across diverse industries such as higher education, governmental organizations, energy, healthcare, manufacturing and telecommunications, with special focus on large multi-national banking institutions. Additionally, he has worked with many international law firms in several international locales that include Europe and the Middle East.

John served numerous times as an expert witness in the fields of computer forensics and cybersecurity in both federal and state courts and was called upon many times to communicate with the court through written deposition, affidavit and declaration.

John's articles have been featured in various publications on topics relating to cyber security and cyberthreats, including a recent article published by the Chief Privacy Officer Magazine. In addition to this, John has also been invited to speak at various notable universities and conferences and served a member of the cyber security advisory board for the Southern Methodist University in Dallas.

Stay Ahead with KROLL

Risk and Financial Advisory Solutions

6,500 professionals worldwide
Continuing the firm's nearly 100-year history of trusted expertise

Unique insights, data and technology
Providing foresight clients need to create an enduring competitive advantage

1 **Valuation**

Valuation of businesses, assets and alternative investments for financial reporting, tax and other purposes.

2 **Compliance and Regulation**

End-to-end governance, advisory and monitorship solutions to detect, mitigate and remediate operational security, legal, compliance and regulatory risk.

3 **Corporate Finance and Restructuring**

Comprehensive corporate finance, investment banking and restructuring support to clients, investors and stakeholders.

4 **Cyber Risk**

Incident response, digital forensics, breach notification, managed detection services, penetration testing, cyber assessments and advisory.

5 **Environmental, Social and Governance**

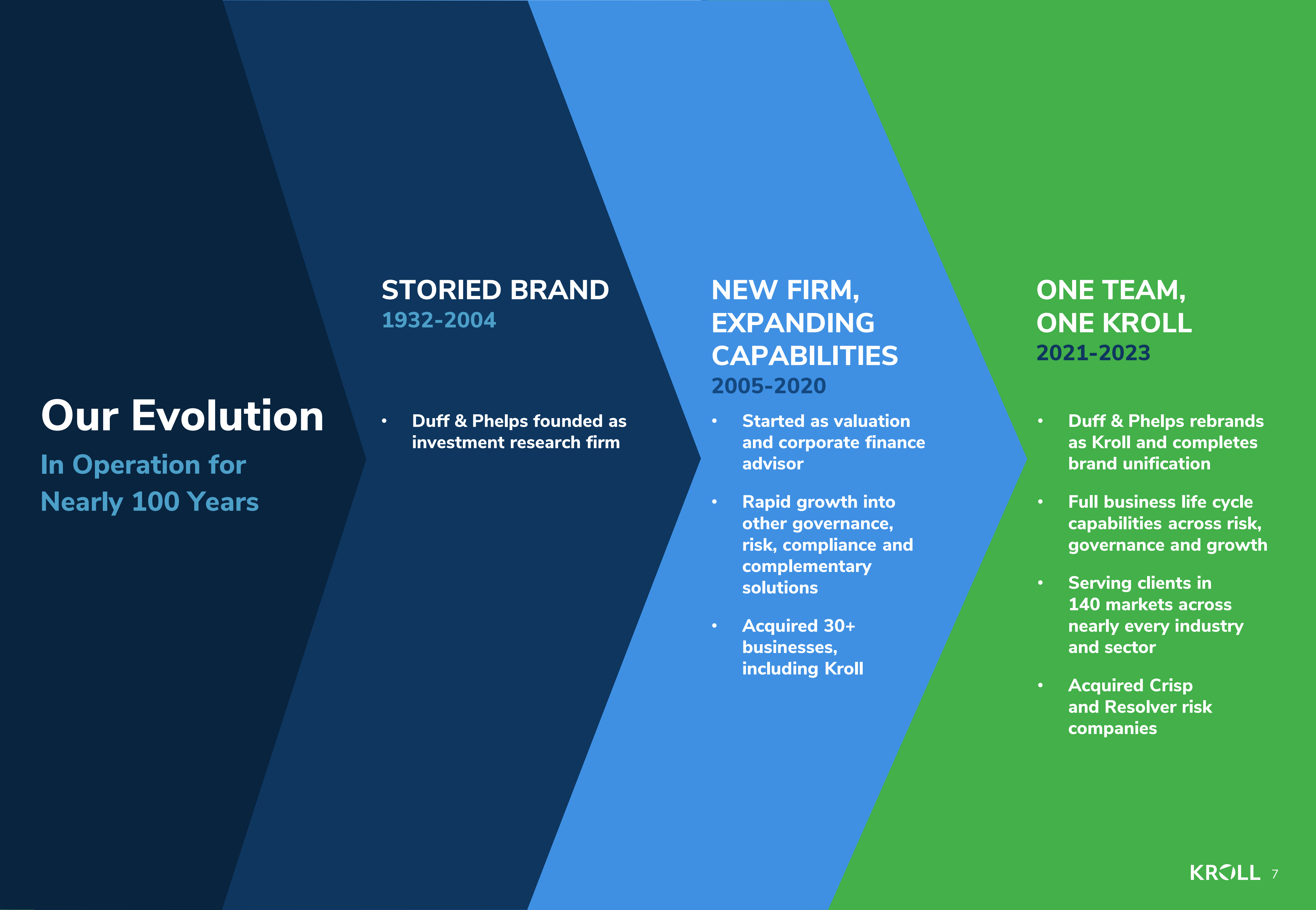
Solutions include policies and procedures, screening and due diligence, disclosures and reporting and investigations, value creation and monitoring.

6 **Investigations and Disputes**

Worldwide expert services and tech-enabled advisory through all stages of diligence, forensic investigation, litigation and testimony.

7 **Business Services**

Technology-enabled legal and business solutions for corporate restructurings, settlement administrations, issuer services, agent and trustee services and other complex support needs.



Our Evolution

In Operation for Nearly 100 Years

STORIED BRAND

1932-2004

- Duff & Phelps founded as investment research firm

NEW FIRM, EXPANDING CAPABILITIES

2005-2020

- Started as valuation and corporate finance advisor
- Rapid growth into other governance, risk, compliance and complementary solutions
- Acquired 30+ businesses, including Kroll

ONE TEAM, ONE KROLL

2021-2023

- Duff & Phelps rebrands as Kroll and completes brand unification
- Full business life cycle capabilities across risk, governance and growth
- Serving clients in 140 markets across nearly every industry and sector
- Acquired Crisp and Resolver risk companies

Our Values

Excellence
Excellence is a mindset – we do challenging work and pursue extraordinary results. We relentlessly focus on excellence – for our clients and colleagues.

Ambition
We are energized to learn, to teach, to grow. We constantly seek to do better – comfort and excellence rarely co-exist.

Courage
We make bold decisions, not just the easy ones. We find, reveal and tell the truth. Integrity is the foundation of everything we do.

Inclusion
We embrace and cultivate diversity – we respect, include and value one another. We support and care about the communities where we live and work.

Innovation
We challenge ourselves to discover new ways to create value. We harness the power of smart data with technology to enable faster decisions and always anticipate what's next for our clients.

One Team, One Kroll
We are stronger together – always focused on solutions, not silos. We collaborate across borders and disciplines in pursuit of excellence.

Excellence
Ambition
Courage
Inclusion
Innovation
ONE TEAM,
ONE
KROLL

Awards and Rankings

We Work with

- 51% of the S&P 500 companies
- 68% of Fortune 100 companies
- 93% of Am Law 100 law firms
- 20 of the 25 largest Euro STOXX® companies
- 69% of the 100 largest Euro STOXX® companies
- The 25 largest private equity firms in the PEI 300
- 21 of the 25 largest hedge funds in the Alpha Hedge Fund 100

Unique Perspective on Deal and Valuation Trends

REFINITIV

Refinitiv Global M&A Review 2021

- 2021 Ranked #1 for Announced Fairness Opinions in the U.S., EMEA and globally
- Ranked #5 for U.S. Middle-Market Transactions over the past 10 years*

**Refinitiv Data (U.S. deals \$10M < \$170M, including deals without a disclosed value.) Full years 2012 through 2021.*

privateequitywire

Private Equity Wire US Awards 2022

- Kroll Wins Best Regulatory and Compliance Firm of the Year

Broad Risk Prevention and Resolution

WWL

Who's Who Legal (WWL) 2022

- Experts recognized in WWL Asset Recovery, Construction – Quantum Delay & Technical, Forensic Accountants Quantum of Damages

GIR Global Investigations Review

Global Investigations Review (GIR) 100 2021

- Named as one of the top 100 cross-border investigations practices

tri TURNAROUND, RESTRUCTURING AND INSOLVENCY

Turnaround, Restructuring & Insolvency Awards 2021

- **Winner** - Turnaround Firm of the Year

GAR Global Arbitration Review

Global Arbitration Review's GAR 100 Expert Witness Firms Power Index - 2022

- Ranked fifth on the annual list of top expert firms globally.

Recognized Cyber Solutions

FORRESTER®

Forrester Wave^{TM} 2022

- Kroll named a Strong Performer in the Forrester Wave^{TM} Cybersecurity Incident Response Services Q1 2022

SC 2022 awards EUROPE

SC Awards Europe 2022

- **Winner** - Managed Detection and Response Solution
- **Finalist** - Best Incident Response Solution

IDC

IDC MarketScape 2021

- Named a Global Leader in Incident Response Readiness

“Facts are stubborn things; and whatever may be our goals, our inclinations, or the dictates of our strategy, these cannot alter the state of facts and evidence.”

- John Adams

KROLL

Board of Directors – Cyber Risk Responsibilities

Board of Directors – Cyber Risk Responsibilities

The SEC forcing the boardroom to change how it does business

Regulation of Investment Advisers

In February 2022, the SEC proposed its first-ever cybersecurity rules for registered investment advisers ("RIAs") (including RIAs to private funds) and Funds (which include registered investment companies ("RICs") and closed-end funds that have elected to be treated as business development companies ("BDCs") under the Investment Company Act. The SEC has indicated that it plans to issue final rules in April 2023

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

On March 9, 2022, the SEC released its newest series of proposed cybersecurity rules, this time for all public companies. Consistent with the proposed rules last issued for investment advisers and funds. The SEC continues to prioritize cybersecurity disclosures to the marketplace, placing particular emphasis on timely and detailed disclosures of material cybersecurity incidents, as well as on periodic disclosures about cybersecurity risk management and governance.

APRIL 2023

Regulation of Investment Advisers

1. **48-Hour Breach Notification Deadline**
   Registrants must implement clear protocols for reporting incidents internally, drafting incident notifications, and obtaining the necessary approvals to send out their notifications within the deadline.
2. **Cybersecurity Policies & Procedures**
   Registrants must ensure that the required policies and procedures are implemented or that their current policies and procedures encompass all requirements provided in the Proposed Rules. Registrants should look to their risk assessment procedures to ensure that they are identifying, categorizing, and prioritizing cybersecurity risks presented by their systems and operations.
3. **Disclosure Obligations**
   Registrants should have a system by which to update such disclosures as new facts come to light, including the provision of certain disclosures associated with cybersecurity risks or incidents to the SEC as well as to clients, investors, and other market participants.
4. **Maintain Fidelity of Operations During an Incident**
   Registrants must consider testing their incident response and business continuity plans through tabletop exercises, to see if they are current and actionable with a focus on the importance of continued operations in the event of a cybersecurity incident.
5. **Documentation**
   Registrants must maintain well-documented evidence that its cybersecurity program has been, and remains, compliant.

APRIL 2023

Registrant Rules for Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

1. **Incident Response Planning**
   Registrants should review their incident response plans to ensure that they contain an escalation path to the legal and executive teams responsible for assessing materiality.
2. **Assess Materiality Thresholds**
   Registrants must understand the costs of what could go wrong before the incident and must establish thresholds for materiality in advance, allowing the company to focus its resources on restoration and mitigation when the incident occurs.
3. **Prepare Templates**
   Registrants must consider what language, delivery format and notification thresholds they can prepare in advance of any incident.
4. **Disclosures and Evidence Preservation**
   Registrants must ensure that their disclosures are not only accurate, but also are supported by objective evidence and documentation, which will require some thoughtful analysis as to over which aspects of the investigation the company wishes to maintain and assert privilege.
5. **Test and Train at All Levels**
   Registrants should consider including both management and the board in tabletop exercises, allowing these key players an opportunity to better understand their roles and responsibilities before, during, and after a cybersecurity incident.
6. **De Facto Cybersecurity Standards**
   Registrants should consider evaluating their cybersecurity programs against known industry standards in anticipation of such public disclosures and take appropriate steps to align their practices.

Cybersecurity Strategy Roadmap

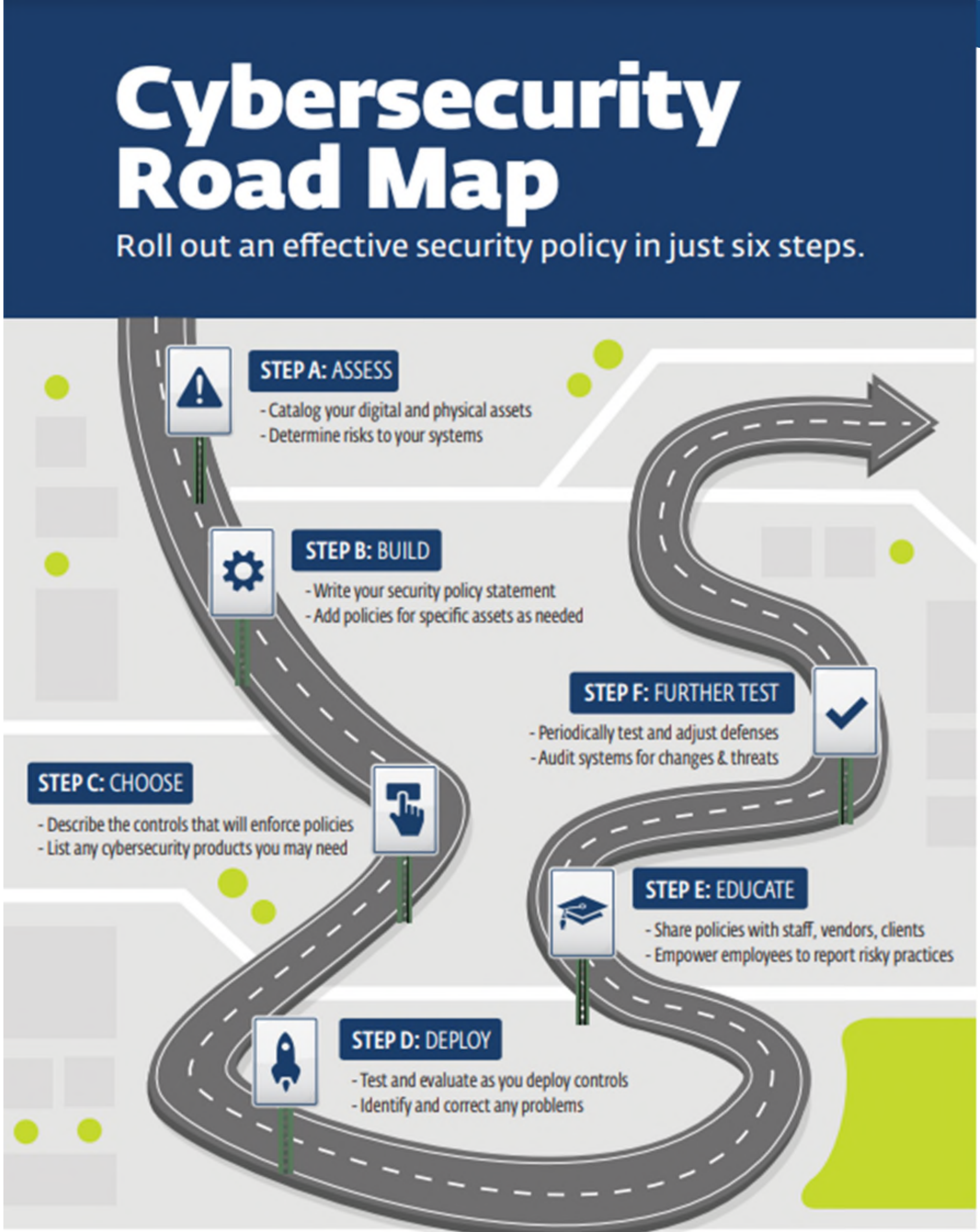
Cyber Road-Mapping

Keep It On The Road!

Methodology

A methodology is not a roadmap

- Understand, document, and monitor your organization’s landscape.
  - Asset Inventory management
- Roadmaps are anchored: Determine a framework or set of standards to adhere to
  - Regulations | Frameworks | Standards | Control Sets
  - So that a comprehensive strategy can be created
- Benchmark your cyber security performance through testing and assessments
- Define your gaps according to the framework, regulatory requirements, and standards
- Prioritize your investments and remediation in alignment with the goals of the business
- Communicate the state of security
- Continuous Improvement Plan



Cybersecurity Road Map

Roll out an effective security policy in just six steps.

STEP A: ASSESS

- Catalog your digital and physical assets
- Determine risks to your systems

STEP B: BUILD

- Write your security policy statement
- Add policies for specific assets as needed

STEP C: CHOOSE

- Describe the controls that will enforce policies
- List any cybersecurity products you may need

STEP D: DEPLOY

- Test and evaluate as you deploy controls
- Identify and correct any problems

STEP E: EDUCATE

- Share policies with staff, vendors, clients
- Empower employees to report risky practices

STEP F: FURTHER TEST

- Periodically test and adjust defenses
- Audit systems for changes & threats

https://www.eset.com/us/business/resources/infographics/cybersecurity-roadmap/

NIST CYBERSECURITY FRAMEWORK (CSF)

Industry Standard Benchmark to Evaluate an Information Security Program

IDENTIFY

the assets that need protection

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Supply Chain Risk Management

PROTECT

against incidents by implementing risk-based safeguards

- Identity Management, Authentication and Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

DETECT

and identify suspicious activity by monitoring enterprise

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

RESPOND

effectively to contain an incident

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

and restore systems or assets affected by an incident

- Recovery Planning
- Improvements
- Communications

NIST CYBERSECURITY FRAMEWORK

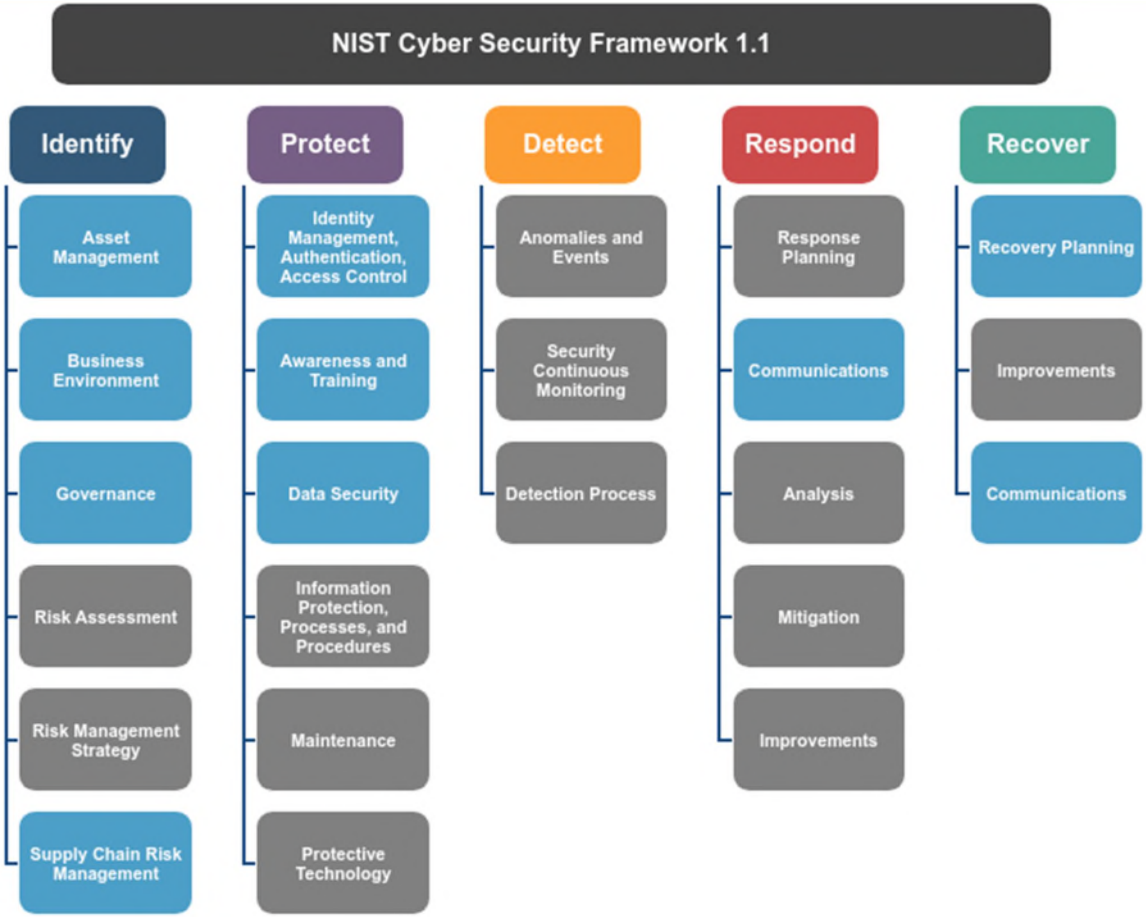
Implementation Status

The **NIST cybersecurity framework** helps organizations understand their cybersecurity risks (**threats, vulnerabilities and impacts**) and how to reduce these risks using a set of guidelines and best practices to help organizations build and improve their cybersecurity posture. The framework puts forth a set of recommendations and standards that enable organizations to **be better prepared** in identifying and detecting cyber-attacks, and provides guidelines on how to **respond, prevent, and recover from cyber incidents.**

The NIST Framework includes five functions (**Identify, Protect, Detect, Respond, and Recover**) which represent pillars for a successful and holistic security program.

Kroll has assigned [redacted] a color-coded Implementation Status for each NIST subcategory based on Kroll's observations during the risk assessment:

- Gray = Not Implemented
- Light Blue = Partially Implemented
- **Dark Blue** = Fully Implemented
- **Off-White** = Not Assessed



NIST Cyber Security Framework 1.1

Identify
- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Supply Chain Risk Management

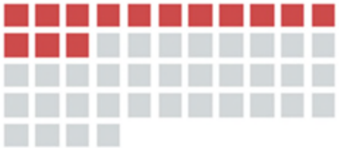
Protect
- Identity Management, Authentication, Access Control
- Awareness and Training
- Data Security
- Information Protection, Processes, and Procedures
- Maintenance
- Protective Technology

Detect
- Anomalies and Events
- Security Continuous Monitoring
- Detection Process

Respond
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover
- Recovery Planning
- Improvements
- Communications

NIST CSF SUMMARY OF FINDINGS

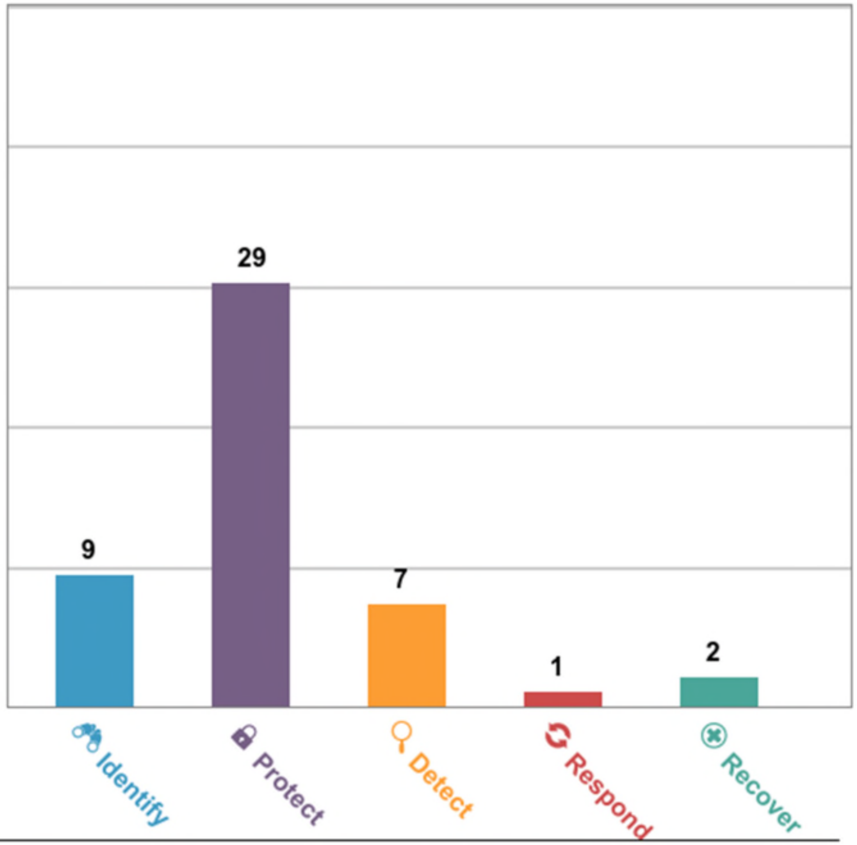


14 HIGH RISK FINDINGS that may cause extensive harm to the organization – these should be addressed immediately

34 MEDIUM RISK FINDINGS that may lead to significant harm to the organization – these should be assessed, prioritized and remediated as quickly as possible

0 LOW RISK FINDINGS that identify opportunities to strengthen the overall security posture of the organization through low-cost and low-impact modifications to the existing security posture – these should be remediated according to standard maintenance windows

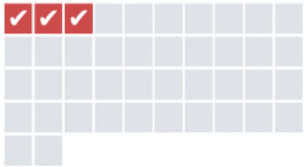
NIST CSF FINDINGS BY CATEGORY



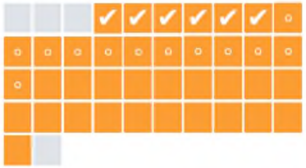
KROLL
BUSINESS SERVICES

Cyber Risk: 42 Findings - High, Medium & Low

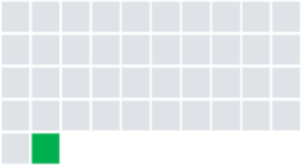
✓ Complete ○ In Progress ■ Not Started



3 HIGH RISK known to cause extensive harm to the organization; should be addressed immediately



38 MEDIUM RISK that could lead to significant harm to the organization; should be assessed, prioritized and remediated as quickly as possible



1 LOW RISK that identify opportunities to strengthen the overall security posture of the organization through low-cost and low-impact modifications to existing security posture; should be remediated according to standard maintenance windows

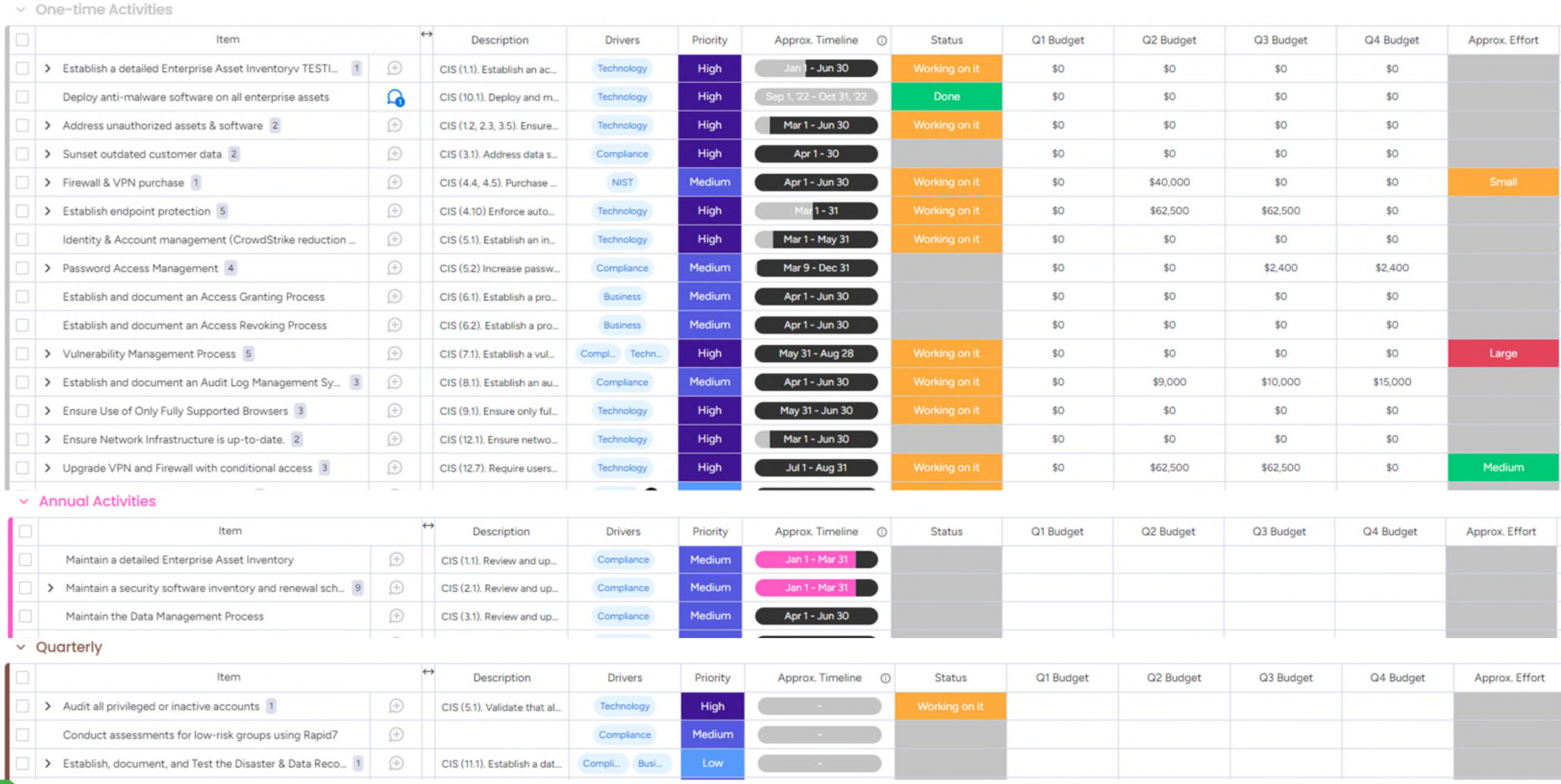
1. Crowdstrike Endpoint Detection proactively monitored 24/7 by Falcon Complete
2. End-of-life MacOS systems (6) replaced
3. The use of external Universal Serial Bus (USB) devices such as smartphones, hard drives and thumb drives is restricted
4. Implemented formal audit of active user, privileged user, or cloud services accounts to identify accounts for individuals who have departed
5. Establish a formal process to inform the business of accepted or remediated information security risks
6. Adopt and test a cyber incident response plan
7. Regular rotation of access keys for Amazon Web Services (AWS) infrastructure
8. Establish a third party risk management program
9. Establish a formal Disaster Recovery Plan

All **medium** risk items will be addressed to an acceptable level by _______ standards by the end of 2023.

Prioritizing the Roadmap

Finding	Probability	Impact	Overall Risk Score	Recommendation
Endpoint protection is not installed consistently across the organization.	High	High	High	Ensure Bitdefender endpoint security is installed and configured on all workstations and servers to protect against viruses and malware.
There is no formal process for applying security updates to servers, network infrastructure, or databases; patching is ad-hoc.	High	High	High	Implement a formal schedule for applying any Critical or High rated security updates on at least a monthly basis. Deploy patches through a centralized management solution (NinjaOne, Microsoft WSUS, InTune) or provider (Automox). The patch management process should include acquiring, testing, and installing application, system, and firmware updates. Require scheduled system reboots to ensure patches are fully applied. Patches that are not fully applied will block the application of future updates.
Virtual private network (VPN) remote access does not require multi-factor authentication.	High	High	High	Implement multi-factor authentication (MFA) using authenticator applications for all remote access methods into the organization's systems, cloud services, and networks. MFA dramatically reduces the risk of attackers compromising the organization's private networks utilizing stolen credentials (e.g., from a successful phishing campaign). Use hardware (FIDO) keys where available, as other factor methods of MFA may be more susceptible to Adversary-in-the-Middle (AitM) attacks.
Critical production workloads rely on end-of-life products (e.g., VMware 5.5, Windows 2012, CentOS 5, PostgreSQL 8. x ,Windows 10 1803 & 1909, CentOS 5.11).	High	High	High	Replace or upgrade any system not running a supported product or implement sufficient controls to reduce the likelihood that an attacker may compromise the system. Countermeasures such as network segmentation or endpoint detection and response (EDR) applications reduce the risk of exploitation of end-of-life system vulnerabilities.

Prioritizing the Roadmap



One-time Activities

□	Item	Description	Drivers	Priority	Approx. Timeline	Status	Q1 Budget	Q2 Budget	Q3 Budget	Q4 Budget	Approx. Effort
□	Establish a detailed Enterprise Asset Inventoryv TESTI... 1	CIS (1.1). Establish an ac...	Technology	High	Jan 1 - Jun 30	Working on it	$0	$0	$0	$0	
□	Deploy anti-malware software on all enterprise assets	CIS (10.1). Deploy and m...	Technology	High	Sep 1, '22 - Oct 31, '22	Done	$0	$0	$0	$0	
□	Address unauthorized assets & software 2	CIS (1.2, 2.3, 3.5). Ensure...	Technology	High	Mar 1 - Jun 30	Working on it	$0	$0	$0	$0	
□	Sunset outdated customer data 2	CIS (3.1). Address data s...	Compliance	High	Apr 1 - 30		$0	$0	$0	$0	
□	Firewall & VPN purchase 1	CIS (4.4, 4.5). Purchase ...	NIST	Medium	Apr 1 - Jun 30	Working on it	$0	$40,000	$0	$0	Small
□	Establish endpoint protection 5	CIS (4.10) Enforce auto...	Technology	High	Mar 1 - 31	Working on it	$0	$62,500	$62,500	$0	
□	Identity & Account management (CrowdStrike reduction ...	CIS (5.1). Establish an in...	Technology	High	Mar 1 - May 31	Working on it	$0	$0	$0	$0	
□	Password Access Management 4	CIS (5.2) Increase passw...	Compliance	Medium	Mar 9 - Dec 31		$0	$0	$2,400	$2,400	
□	Establish and document an Access Granting Process	CIS (6.1). Establish a pro...	Business	Medium	Apr 1 - Jun 30		$0	$0	$0	$0	
□	Establish and document an Access Revoking Process	CIS (6.2). Establish a pro...	Business	Medium	Apr 1 - Jun 30		$0	$0	$0	$0	
□	Vulnerability Management Process 5	CIS (7.1). Establish a vul...	Compl... Techn...	High	May 31 - Aug 28	Working on it	$0	$0	$0	$0	Large
□	Establish and document an Audit Log Management Sy... 3	CIS (8.1). Establish an au...	Compliance	Medium	Apr 1 - Jun 30	Working on it	$0	$9,000	$10,000	$15,000	
□	Ensure Use of Only Fully Supported Browsers 3	CIS (9.1). Ensure only ful...	Technology	High	May 31 - Jun 30	Working on it	$0	$0	$0	$0	
□	Ensure Network Infrastructure is up-to-date. 2	CIS (12.1). Ensure netwo...	Technology	High	Mar 1 - Jun 30		$0	$0	$0	$0	
□	Upgrade VPN and Firewall with conditional access 3	CIS (12.7). Require users...	Technology	High	Jul 1 - Aug 31	Working on it	$0	$62,500	$62,500	$0	Medium

Annual Activities

□	Item	Description	Drivers	Priority	Approx. Timeline	Status	Q1 Budget	Q2 Budget	Q3 Budget	Q4 Budget	Approx. Effort
□	Maintain a detailed Enterprise Asset Inventory	CIS (1.1). Review and up...	Compliance	Medium	Jan 1 - Mar 31						
□	Maintain a security software inventory and renewal sch... 9	CIS (2.1). Review and up...	Compliance	Medium	Jan 1 - Mar 31						
□	Maintain the Data Management Process	CIS (3.1). Review and up...	Compliance	Medium	Apr 1 - Jun 30						

Quarterly

□	Item	Description	Drivers	Priority	Approx. Timeline	Status	Q1 Budget	Q2 Budget	Q3 Budget	Q4 Budget	Approx. Effort
□	Audit all privileged or inactive accounts 1	CIS (5.1). Validate that al...	Technology	High	-	Working on it					
□	Conduct assessments for low-risk groups using Rapid7		Compliance	Medium	-						
□	Establish, document, and Test the Disaster & Data Reco... 1	CIS (11.1). Establish a dat...	Compli... Busi...	Low	-						

Quarterly Roadmap

Q1

- ✓ Weekly Security Meeting Established
- Cyber Insurance Policy
- ✓ Migration of .com to .net
- Firewall purchase & Implementation ($100k)
- VPN Upgrade with conditional formatting
- Intune Pilot Deployed
- Mobile and BYOD policy finalized
- Data Removal process fully documented with a corresponding retention policy
- Rapid 7 full deployment
- Scanning policies and procedures
- Global Security Plan & Presentation
- Client communications

Q2

- ISO Certification Renewed
- Update of Security Policies
- Analysis and Decision on Google to 0365 Implementation
- Elimination of all unnecessary client data
- Full patch management policy and plan
- End Point Protection fully implemented and managed by Intune
- Standardize supported application inventory
- Penetration Test external in and internal out.
- CrowdStrike risk rating reduced to less than 4

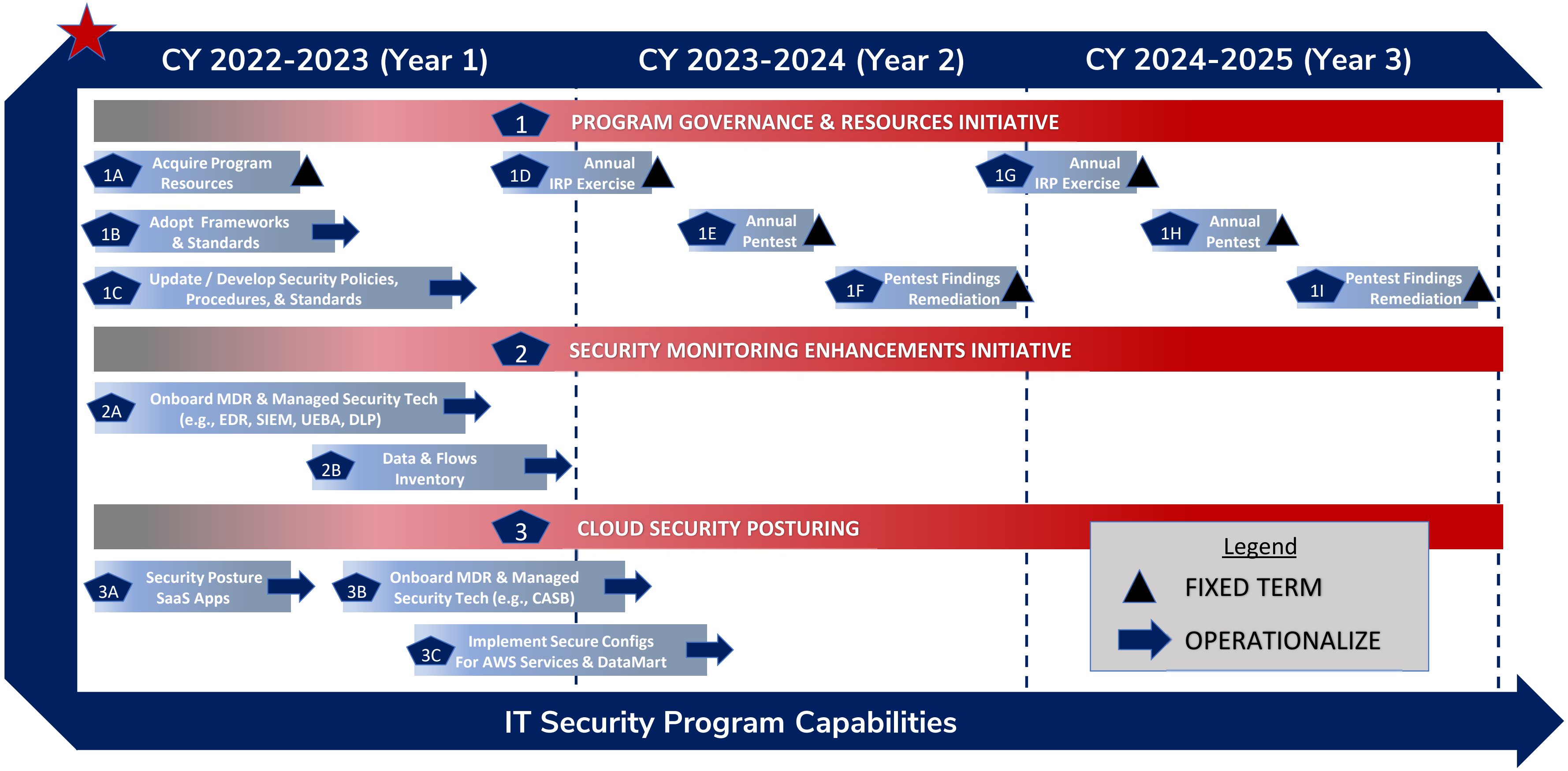
Q3

- Full Risk Assessment (including security audit of server infrastructure)
- Google Environment Assessment
- Azure Security Assessment
- Jira/Confluence/Stash and other web apps Assessment
- Full testing of IRP and TTX Exercises
- Third Party Risk Assessment Framework
- Implementation of automated patch management solution
- Quarterly report produced by Data Dog
- Full inventory system in accordance with CIS v8
- Full risk register and remediation tracker

Q4

- Renewal of CrowdStrike
- Renewal of Rapid 7
- Renewal of Data Dog
- Enhanced Security Awareness Training (KnowBe4)
- Policy Management Solution (Tugboat Logic)

Initiatives Roadmap



CY 2022-2023 (Year 1)

CY 2023-2024 (Year 2)

CY 2024-2025 (Year 3)

1 PROGRAM GOVERNANCE & RESOURCES INITIATIVE

1A Acquire Program Resources ▲

1B Adopt Frameworks & Standards ➡

1C Update / Develop Security Policies, Procedures, & Standards ➡

1D Annual IRP Exercise ▲

1E Annual Pentest ▲

1F Pentest Findings Remediation ▲

1G Annual IRP Exercise ▲

1H Annual Pentest ▲

1I Pentest Findings Remediation ▲

2 SECURITY MONITORING ENHANCEMENTS INITIATIVE

2A Onboard MDR & Managed Security Tech (e.g., EDR, SIEM, UEBA, DLP) ➡

2B Data & Flows Inventory ➡

3 CLOUD SECURITY POSTURING

3A Security Posture SaaS Apps ➡

3B Onboard MDR & Managed Security Tech (e.g., CASB) ➡

3C Implement Secure Configs For AWS Services & DataMart ➡

Legend

▲ FIXED TERM

➡ OPERATIONALIZE

IT Security Program Capabilities

● Priority 1 (P1) Initiatives

Cyber Assessment Process

Cybersecurity Assessments – What and When

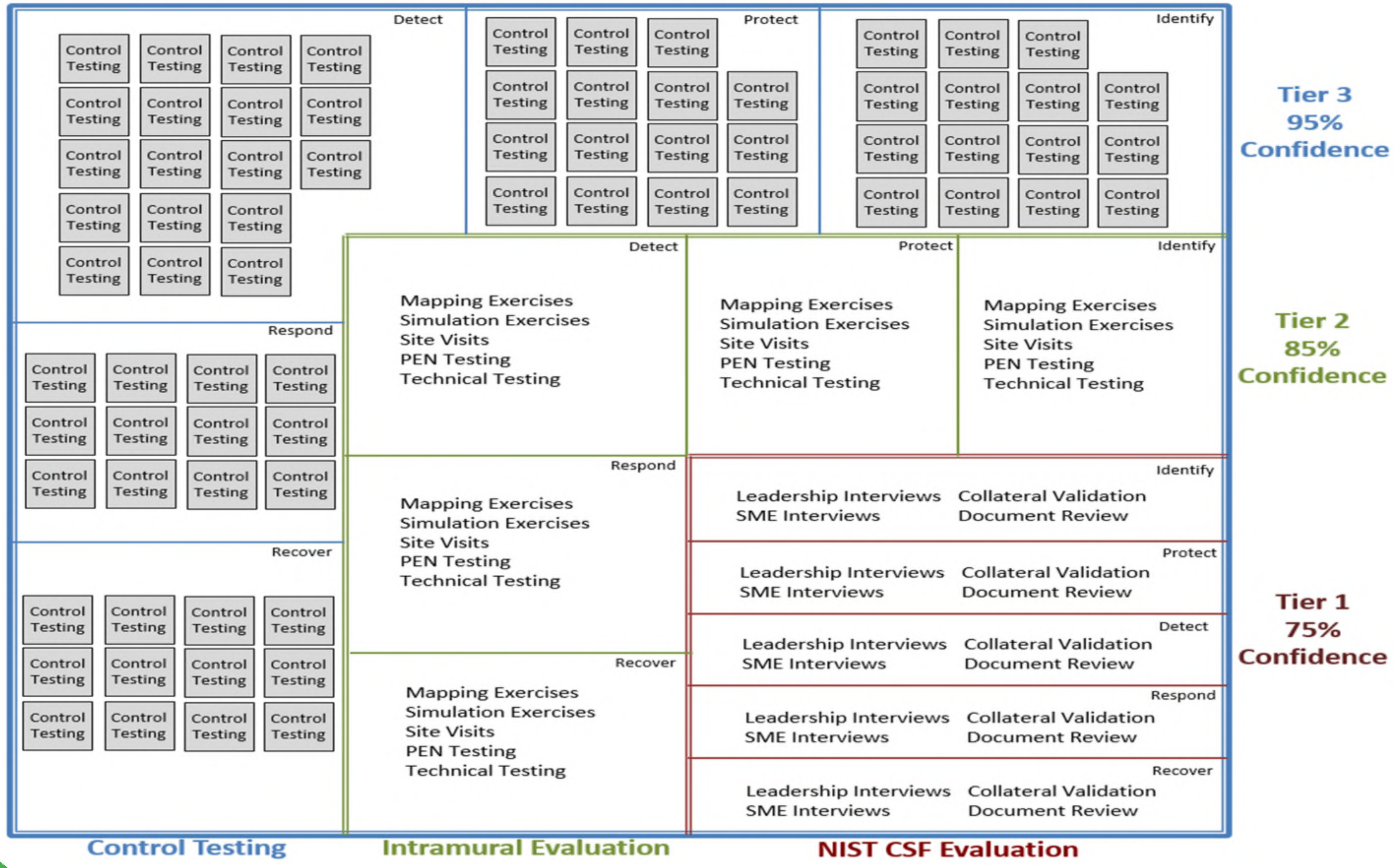
Cybersecurity Assessment Types

- Cyber Program Maturity (NIST CMMC)
- Cyber Program Posture (NIST CSF)
- Incident Response Preparedness
- Regulatory (NYDFS, SEC, FFEIC, DFARS)
- Risk Identification \ Quantification
- Written Information Security Program (WISP)
- Technical Assessments
  - Vulnerability \ PEN Test
  - Internal Compromise
  - App Security (Web-Application \ Code Development)
  - Internet of Things \ OT (SCADA)
  - Networking Devices
  - Security Tooling
- Framework Controls (800 Family, CIST18)
- Certification (Soc2T2, ISO, HIPAA)
- Social Engineering
- Red \ Purple Teaming
- Third-Party Risk Management (Supply Chain)
- M&A Due Diligence
- Privacy or Sensitive Data

Cybersecurity Assessment Drivers

- Board or Executive Request
- Regulator Demands
- Response to Cyber Incident
- Reputation – Customer Expectations
- Cybersecurity Insurance Policy Onboarding
- Bug Bounty \ Testing Results
- Litigation Outcome
- Mergers and Acquisitions

Cybersecurity Assessments - Derivation



Detect

Control Testing Control Testing Control Testing Control Testing
Control Testing Control Testing Control Testing Control Testing
Control Testing Control Testing Control Testing Control Testing
Control Testing Control Testing Control Testing
Control Testing Control Testing Control Testing

Protect

Control Testing Control Testing Control Testing
Control Testing Control Testing Control Testing Control Testing
Control Testing Control Testing Control Testing Control Testing
Control Testing Control Testing Control Testing Control Testing

Identify

Control Testing Control Testing Control Testing
Control Testing Control Testing Control Testing Control Testing
Control Testing Control Testing Control Testing Control Testing
Control Testing Control Testing Control Testing Control Testing

Respond

Control Testing Control Testing Control Testing Control Testing
Control Testing Control Testing Control Testing Control Testing
Control Testing Control Testing Control Testing Control Testing

Recover

Control Testing Control Testing Control Testing Control Testing
Control Testing Control Testing Control Testing Control Testing
Control Testing Control Testing Control Testing Control Testing

Detect

Mapping Exercises
Simulation Exercises
Site Visits
PEN Testing
Technical Testing

Protect

Mapping Exercises
Simulation Exercises
Site Visits
PEN Testing
Technical Testing

Identify

Mapping Exercises
Simulation Exercises
Site Visits
PEN Testing
Technical Testing

Respond

Mapping Exercises
Simulation Exercises
Site Visits
PEN Testing
Technical Testing

Recover

Mapping Exercises
Simulation Exercises
Site Visits
PEN Testing
Technical Testing

Identify

Leadership Interviews Collateral Validation
SME Interviews Document Review

Protect

Leadership Interviews Collateral Validation
SME Interviews Document Review

Detect

Leadership Interviews Collateral Validation
SME Interviews Document Review

Respond

Leadership Interviews Collateral Validation
SME Interviews Document Review

Recover

Leadership Interviews Collateral Validation
SME Interviews Document Review

Control Testing

Intramural Evaluation

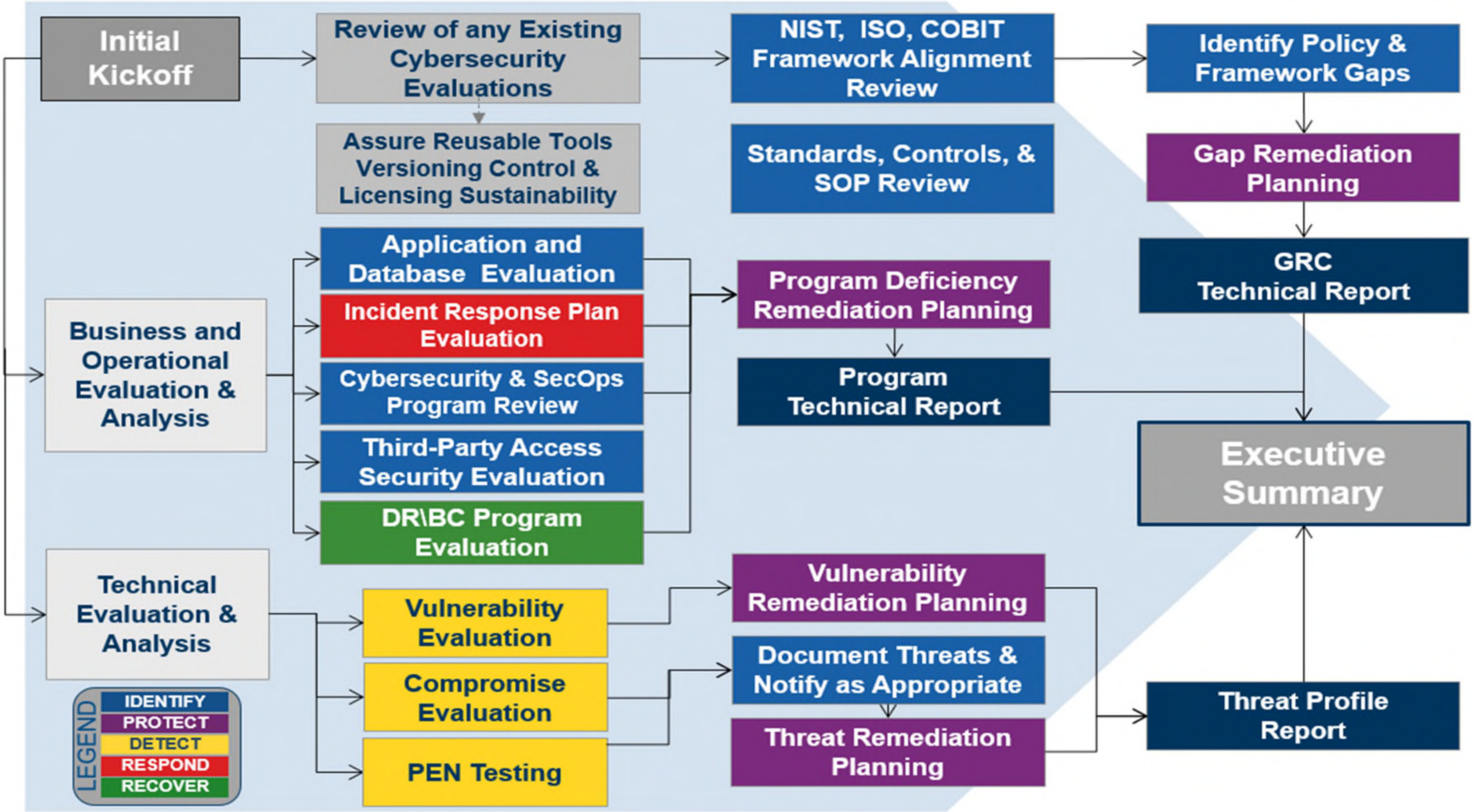
NIST CSF Evaluation

Tier 3
95%
Confidence

Tier 2
85%
Confidence

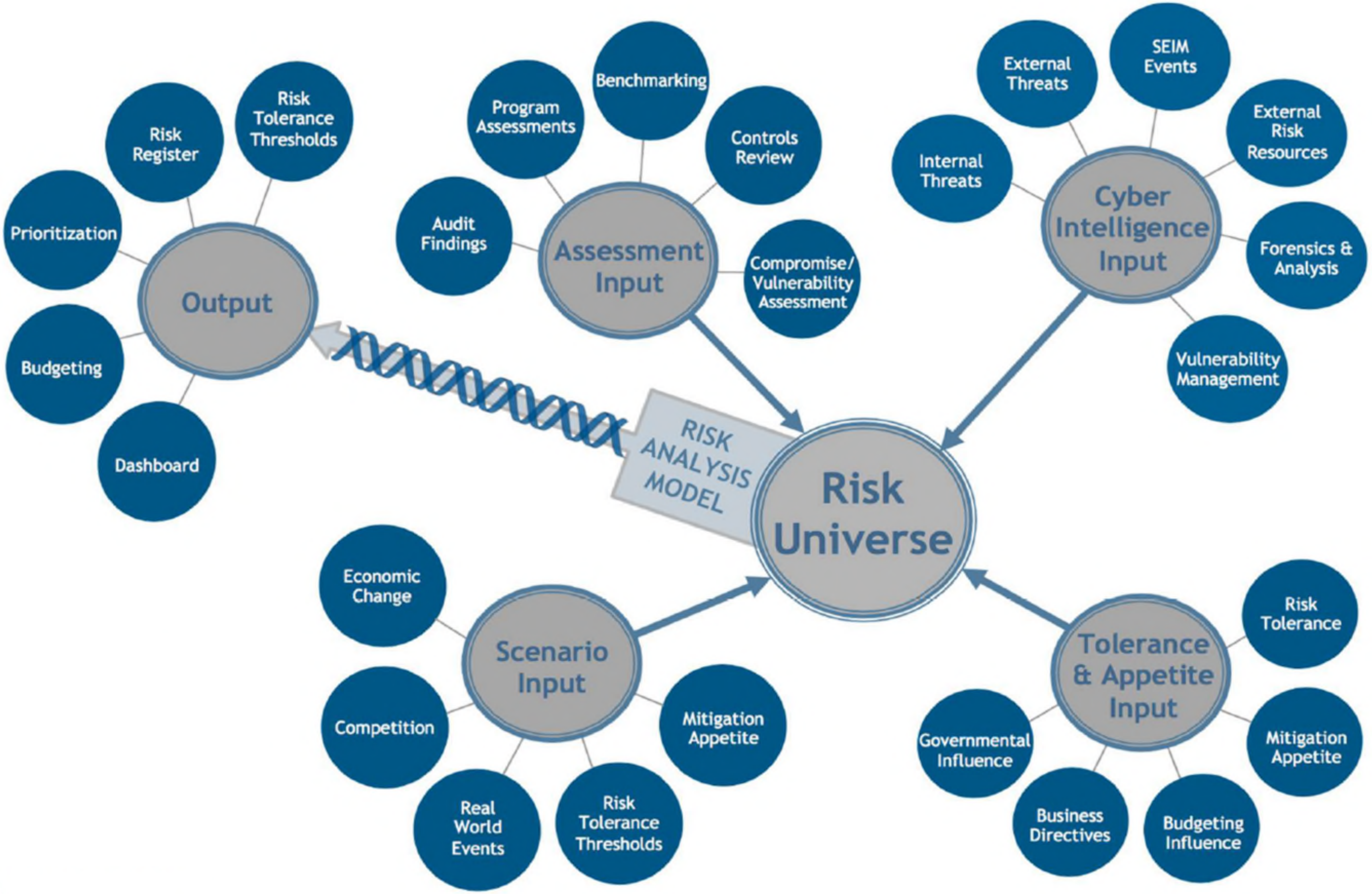
Tier 1
75%
Confidence

Cybersecurity Assessments - How



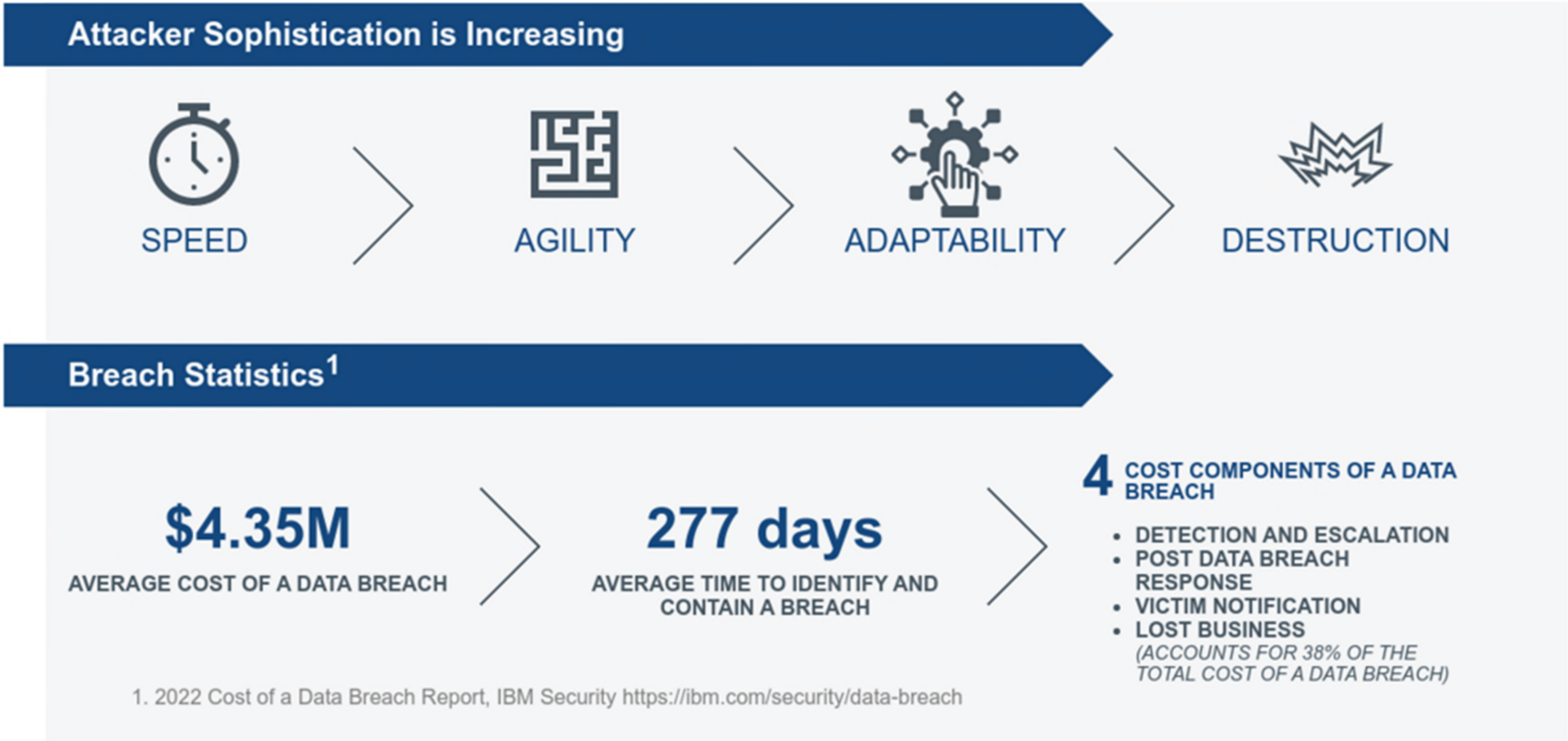
Initial Kickoff
Review of any Existing Cybersecurity Evaluations
NIST, ISO, COBIT Framework Alignment Review
Identify Policy & Framework Gaps
Assure Reusable Tools Versioning Control & Licensing Sustainability
Standards, Controls, & SOP Review
Gap Remediation Planning
GRC Technical Report
Business and Operational Evaluation & Analysis
Application and Database Evaluation
Incident Response Plan Evaluation
Cybersecurity & SecOps Program Review
Third-Party Access Security Evaluation
DR\BC Program Evaluation
Program Deficiency Remediation Planning
Program Technical Report
Executive Summary
Technical Evaluation & Analysis
Vulnerability Evaluation
Compromise Evaluation
PEN Testing
Vulnerability Remediation Planning
Document Threats & Notify as Appropriate
Threat Remediation Planning
Threat Profile Report
LEGEND
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

Cybersecurity Risk Assessment Landscape



M&A Cybersecurity Due Diligence

GLOBAL CYBER THREAT LANDSCAPE



Attacker Sophistication is Increasing

SPEED > AGILITY > ADAPTABILITY > DESTRUCTION

Breach Statistics[1]

$4.35M

AVERAGE COST OF A DATA BREACH

277 days

AVERAGE TIME TO IDENTIFY AND CONTAIN A BREACH

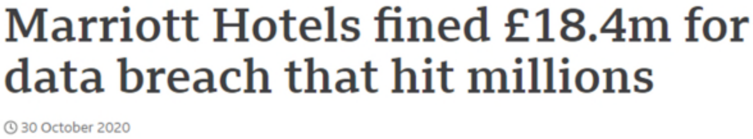
4 COST COMPONENTS OF A DATA BREACH

- DETECTION AND ESCALATION
- POST DATA BREACH RESPONSE
- VICTIM NOTIFICATION
- LOST BUSINESS *(ACCOUNTS FOR 38% OF THE TOTAL COST OF A DATA BREACH)*

[1] 2022 Cost of a Data Breach Report, IBM Security https://ibm.com/security/data-breach

Impact on Deals

Past Deals that have had cyber security components



Marriott Hotels fined £18.4m for data breach that hit millions

30 October 2020

The incident/s occurred both prior to and post acquisition of the Starwood Hotel's Group by Marriott Hotels.

YAHOO!

The purchase price was reduced by $350 million, down to $4.48 billion.

Blackstone KKR THE CARLYLE GROUP TPG WARBURG PINCUS

Advent International APOLLO EnCap Investments L.P. NEUBERGER BERMAN CVC Capital Partners

Outcomes of cyber-DD contribute to reductions in price or have killed deals but are seldom made public!

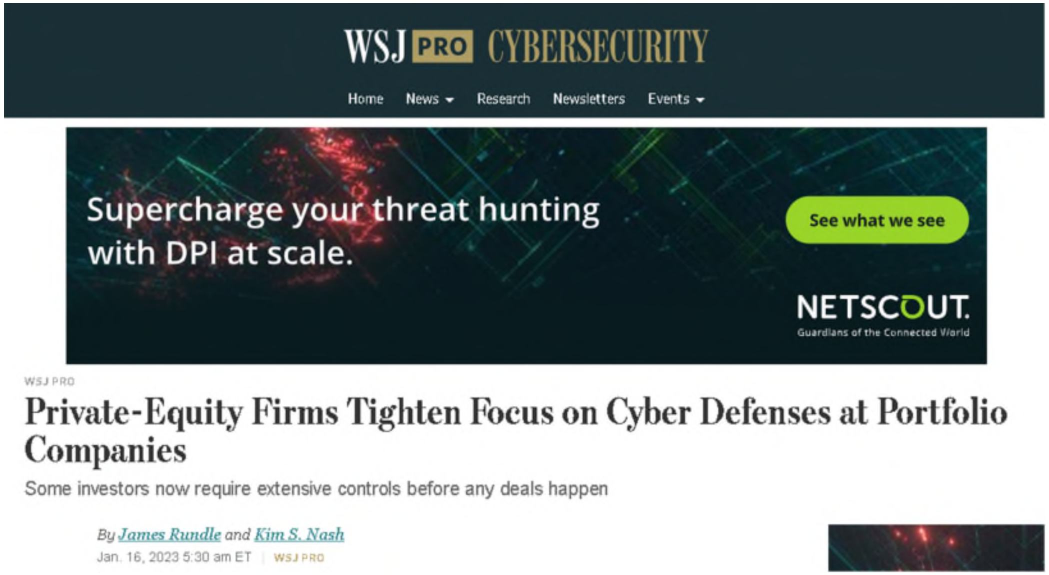
"40% of acquiring businesses find cyber security problems post-transaction"

[Forbes]

REDUCTION IN ASSET VALUE.
BRAND DAMAGE OR SYSTEM OUTAGES.
INHERITING CYBER SECURITY ISSUES OR BREACH FALLOUT.

Private-Equity Firms Tighten Focus on Cyber Defenses at Portfolio Companies

Some investors now require extensive controls before any deals happen



WSJ PRO

Private-Equity Firms Tighten Focus on Cyber Defenses at Portfolio Companies

Some investors now require extensive controls before any deals happen

By James Rundle and Kim S. Nash

Jan. 16, 2023 5:30 am ET | WSJ PRO

Article Here

Both Sides Engage Cyber Support

Sell Side / Vendor Side

The vendor will likely have advanced warning of the sale and will work with the asset to ensure a smooth sale.

Third parties will be engaged to prepare and collate documentation, prepare accounts, and (if needed) coach senior staff.

You never sell a dirty car.

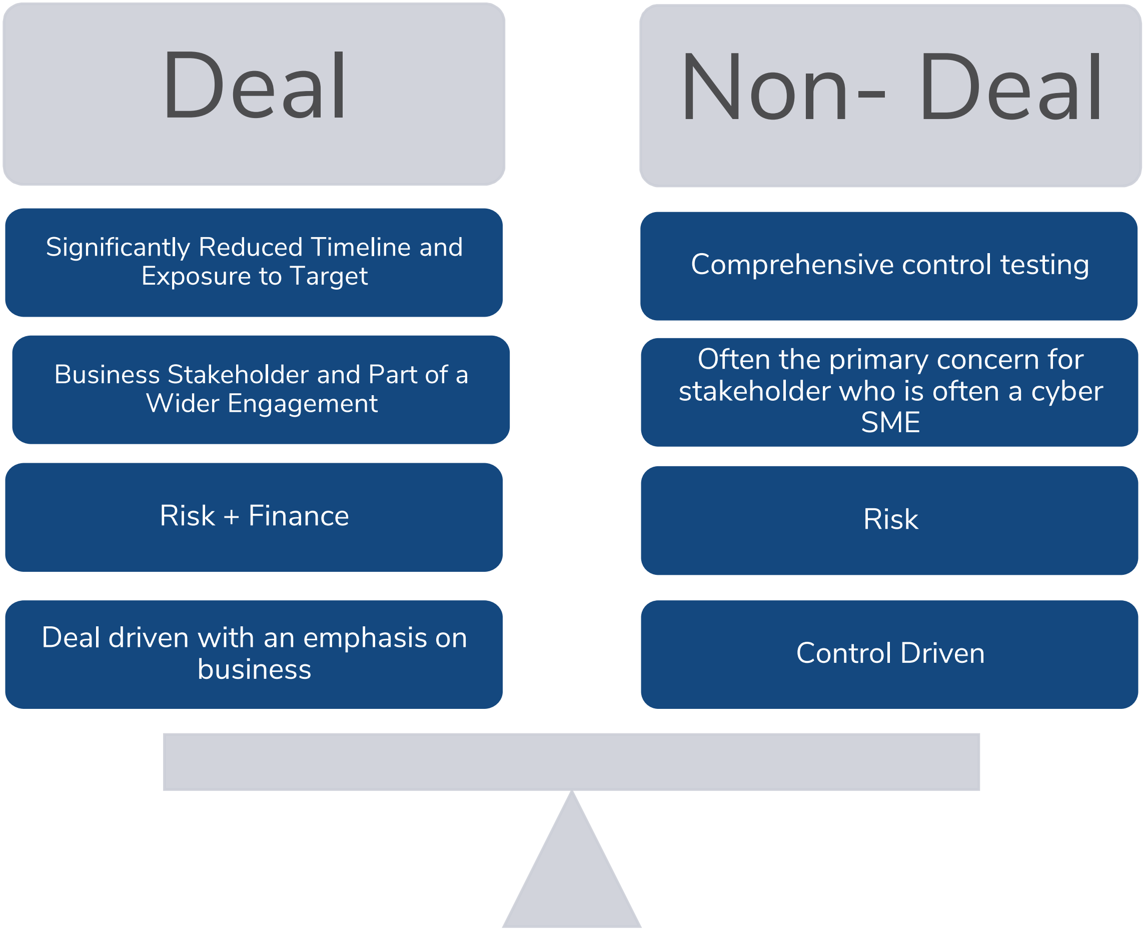
Buy Side

The buy side party will develop their own justification and business case for investment.

The nature and mechanics of the deal will dictate the post acquisition plans and pre/post deal activities offerings.

You never buy a car without lifting the bonnet, looking at the log book.

A DEALS ENGAGEMENT IS NOT A STANDARD CYBER SECURITY CONTROLS ASSESSMENT WITH A REDUCED TIMELINE



Deal	Non- Deal
Significantly Reduced Timeline and Exposure to Target	Comprehensive control testing
Business Stakeholder and Part of a Wider Engagement	Often the primary concern for stakeholder who is often a cyber SME
Risk + Finance	Risk
Deal driven with an emphasis on business	Control Driven

Top Three Concerns (1 of 3)

Should we be going thru with this deal?

1) Tell me “yes or no”
   a. Find a partner that has a background in both cyber AND business
      i. Buyer should look for a partner who “has the license to make this determination”?
         - ○ Importance of interviewing & document review
         - ○ Someone who understands which questions to ask, what not to ask, and how to drive to an answer
   b. Tooling (Dark Web Search, Scanning & Analysis, etc)
      i. IP compromise
      ii. Regulatory Issues
      iii. Legal
      iv. Reputational damage

Question to be answered is: “Is there anything that can undermine this company to the point it can’t succeed?”

Top Three Concerns (2 of 3)

Can the buying price be renegotiated?

1) Can the cost of mitigation and remediation of risk be factored into the negotiated price?
    a. Are there significant costs associated with reducing inherent risk to residual risk?
        i. If your residual risk is at the same level as inherent risk, you have a problem.
        ii. Understand Third Party Risk
2) What controls do they have in place? What are the existing frameworks?
    a. What controls, policies and procedures are missing?
    b. General maturity level?
    c. Why is their maturity level where it is?
        i. Tech Stack?
        ii. Best practices?
3) How early should Cyber DD be brought into the deal process.
    a. Usually brought in very late in the game.
    b. Cyber DD often not given enough time to make remediation/mitigation recommendation and THEN implement them (if you want it prior to the transaction).—Might need to work remediation into the deal

Top Three Concerns (3 of 3)

You need to know the team that you are “buying”

1) Are they competent?

2) Are they fully resourced?

3) Should the buyer bring on additional resources to help?

4) Do people need to be removed/replaced?

5) Do you have the staff to do the recommended remediations?

Kroll Cyber Risk Diligence

Tailored, Project-Based Diligence Engagements

BASE

No involvement required from target; basic level of assurance; minimizes target's awareness of efforts.

- **Dark Web Reconnaissance / Threat Intelligence**
  - – Review Deep and Dark Web data repositories for target's IP, keywords, leaked or lost credentials and data.
- **Digital Footprint / Attack Surface Survey**
  - – Enumeration of externally visible footprint (i.e. attack surface), including hosts, hosting providers, geographies
- **Peer Benchmarking / Security Rating**
  - – External evaluation of 10 security criterion
    - ○ Patching, Application Security, Web Encryption, etc.
  - – Benchmarks include both letter grade (A-F) and peer rank percentage mechanic

Duration	Target Involvement	Cost
5 -10 Days	None	

CORE

Direct interaction with the target; achieves a moderate level of assurance; target made aware of efforts.

Every service from **BASE**, plus:

- **Security Program Maturity Assessment**
  - – Review security documentation (security policies, network architecture diagrams, etc.)
  - – Conduct up to five (5) interviews with IT, InfoSec, Software Development, to better understand governance and risk management posture within the target
  - – Follow-up requests/interviews (if and as necessary)
- **External Vulnerability Scanning**
  - – Scan up to fifty (50) public IP addresses for known vulnerabilities
- **Compensating Controls and Remediation Actions**
  - – Review compensating controls as relates to vulnerabilities discovered during the BASE reconnaissance phase.
  - – Identify top risks and remediation actions (with time & cost)

Duration	Target Involvement	Cost
2 – 4 Weeks	Low – Moderate	

Cyber Risk Diligence

Aggregate Risk: **Moderate**	______was determined to have a MODERATE aggregate risk profile, with a MODERATE inherent risk in the Breach History category.
Diligence Activities	Red Flag Cyber Diligence, Dark Web Review, Interview, Document Review

Key Observations:

- ✓ Based on the dark web search that was conducted as part of the due diligence activity there was no evidence of a significant breach (and subsequent leak) of data or intellectual property having occurred.
- ✓ ______ appears to have minimal tech debt regarding server and network infrastructure and end user devices. ______ costs have generally been operationalized and therefore, should scale with the organization.
- ✓ Software Development Lifecycle is not formally documented; however, ______ follow a release management process and leverages tools to do so. A full Application Development Life Cycle should be implemented increasing controls regarding developers and overall change control. Current development maturity level demonstrated is moderate.
- ✓ Data Loss Protection: The security of company data when it is located on company endpoints is a concern. Data is not encrypted at rest on laptops and desktops.

Risks

1. ____s core business applications are vendor maintained and hosted and the end user authentication is administered individually. There is risk present .
2. Employees use personal mobile device to connect to corporate email and Slack communication channels. Without a Mobile Device Management platform corporate data is exposed.
3. Vendors and contractors are not subjected to information security training nor are their security practices audited on a regular basis.
4. There is no clearly accountable cyber security lead. CTO and GC share the responsibilities of information security.
5. Laptop hard drives are not currently encrypted.
6. Data retention policy does not exist. Current practices leave the organization open to being noncompliant with regulatory requirements such GDPR and CCPA
7. Web management not focused on security. As an example, web sites do not implement one or more important HTTP security headers, patching, and version control issues are present.

Remediation Activities and Costs

1. VCISO: In the short-term (3-6 months) a CISO should be appointed (consultant in the interim while seeking a permanent employee). Eventual expansion to a team of two to three employees. **Cost:$150k – $200k**.
2. Implement Hard Drive Encryption: Immediately, all portable computing devices should have hard drive encryption enabled. This protects data in the event a laptop is lost or stolen. **Cost: $15K - 40K | Timeframe: 2 - 6 weeks.**
3. Create Software Development Lifecycle: Review current practices and formally document the process for all developers to follow when writing and implementing code used by ______. **Cost: $35 - $50K | Timeframe: 1 - 2 mos.**
4. Implement a mobile device manager: Require employees to enroll their device into a corporate management environment to protect data available in email and Slack. **Cost: $25-75K | Timeframe: 2 – 3 mos.**
5. Implementation of SIEM: SIEM can be utilized to monitor all traffic on the corporate network. This will compliment the use of EDR technology to enhance the security posture.
6. Risk Assessment: Conduct a full Cyber Security Assessment which includes a detailed review of the information security program - from policies and procedures to technical controls including People, Process and Technologies. **Cost: $60K - 150K | Timeframe: 2 - 3 months.**
7. Web management practices should be reviewed and incorporated into a formalized security program

Additional findings

Findings	Recommendations	Focus
There is no dedicated cyber security SME within the business, and a heavy reliance is placed on the third party for the provision of security services and those security services are operational services like firewall management or patching	Establish a formal position to oversee the information security program. The individual responsible should have enough knowledge of information security and authority to implement an effective security program. An external third-party could also be engaged to provide Virtual Chief Information Security Officer (vCISO) services.	1
A formal risk management framework and supporting processes which consist of the identification, review and ongoing management of risks is not in place.	A comprehensive cyber security risk management framework such as ISO 31000 or should be chosen and implemented as appropriate.	2
The third-party MSP only covers endpoints, the organisation is not collating data from wider infrastructure and application sources. An initial effort to implement a SIEM is underway, however currently there is no method in place for event correlation and alerting of potential malicious activity.	Implement a Security Information Event Manager (SIEM) to centrally collect, continually correlate, and automatically notify IT staff of potentially adverse events. SIEM data should be stored for a period of no less than eighteen (18) months. This will assist incident response teams in the event of a potential breach to determine the extent and method of attack.	3
No data leakage prevention controls implemented as currently there is no blocking of web-based file sharing services such as Dropbox or ShareFile and the use of external Universal Serial Bus (USB) devices such as smartphones, hard drives, and thumb drives are not restricted.	Implement data leakage controls that limit access to unauthorized third-party file sharing services (e.g., Citrix, Dropbox, Box) and enforce either encryption of data to external hard drives or blocks transferring of data to external hard drives.	4
Back-up and disaster recovery services could be limited and not fully tested for third party solutions. Salesforce is only utilizing native solutions for back-up which may be insufficient.	Ensure all systems and data go through a periodic restore test. System restoration should be validated through multiple parties including users. All systems restores should be aligned with a stated SLA.	5
Indications exist that within the business data is retained beyond what the business requires. An increased volume of data not only directly increases IT hosting overheads, but also places additional pressure on existing cyber security resources to protect data with limited resources.	Adopt a formal Data Retention Policy to govern all aspects of data storage and retention, thereafter, introduce a process for regular data cleansing of data that is no longer required by the organisation.	6

Targetco.

Digital Footprint & Open-Source Intelligence

Target Profile

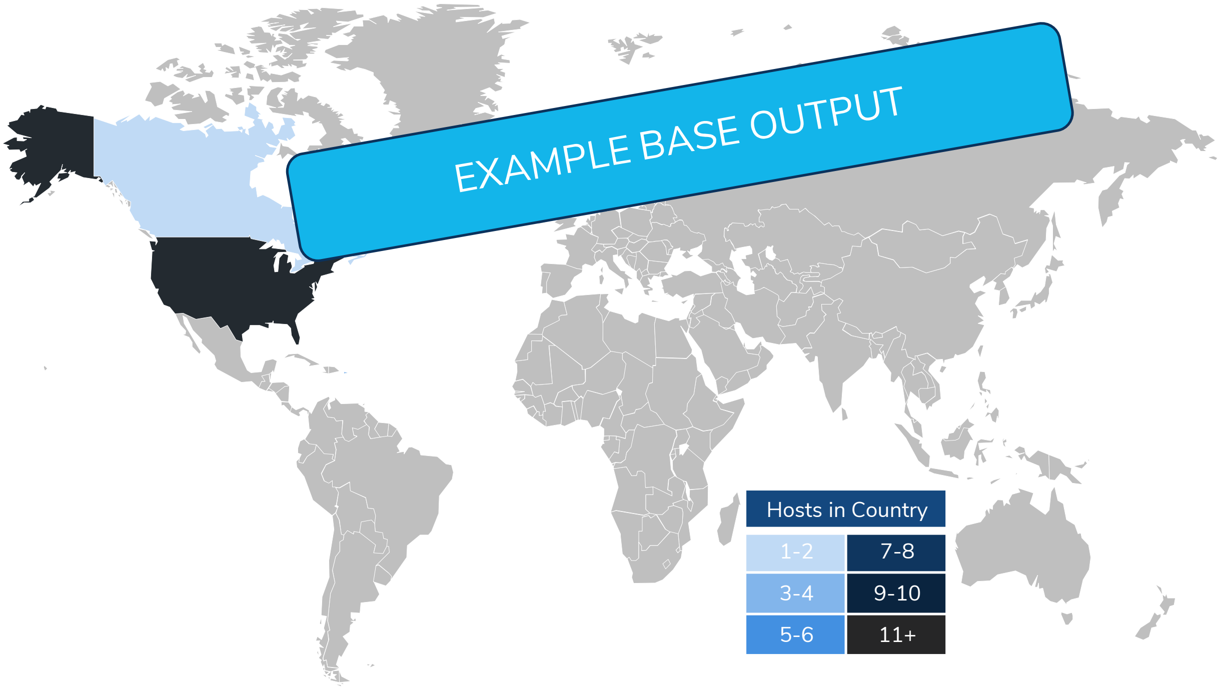
Targetco. is a large technology firm focused on benefits and human resources, based in the United States. They have several data center locations in the following geographies:

- City, State (Provider)
- City, State (Provider)
- City, State (Provider)
- City, State (Provider)

Targetco. employees are largely full-time, with very little contractor utilization.

Digital Footprint

COUNTRY	HOSTS
United States	328
British Virgin Islands	4
Canada	1



RISK CATEGORY	OVERALL	Software Patching	Application Security	Web Encryption	Network Filtering	Email Security	DNS Security	System Hosting
GRADE	A	A	A	B	A	A	A	D
PEER RANK (%ile vs. industry avg.)	97%	100%	94%	86%	100%	100%	100%	17%

Inherent Risk Rating

High-Level Inherent Risk Determination Score

Aggregate Inherent Risk:
MODERATE

_______was determined to have a MOD inherent risk rating. Residual risks can be managed down, but must be done so with intent.

RISK AREA	RISK LEVEL
Industry	High (3)
Breach History	Moderate (2)
Regulated Data Volume	Moderate (2)
Pentest and Findings	Moderate (2)
Post-Trans. Integration	Low (1)
Cyber Maturity	Moderate (2)
Value Proposition	Moderate (2)
Workforce Makeup	Moderate (2)
AGGREGATE TOTAL	MODERATE (16)

Low (8 – 10) Mod. (11 – 17) High (18 – 24)

Dark Web Overview & Open-Source Investigation & Social Media Sentiment

- Kroll Analysts identify the Deep & Dark Web (DDW) as the compilation of sites and sources that include:
  - Community pages such as forums, chat services, blogs, message boards, and paste sites.
  - Cybercriminal pages including ransomware actor-controlled sites.
  - Marketplaces including card shops and account shops where malicious threat actor activity is occurring.

Exposure Risk Rating

De Minimis Risk

Low Risk

Medium Risk

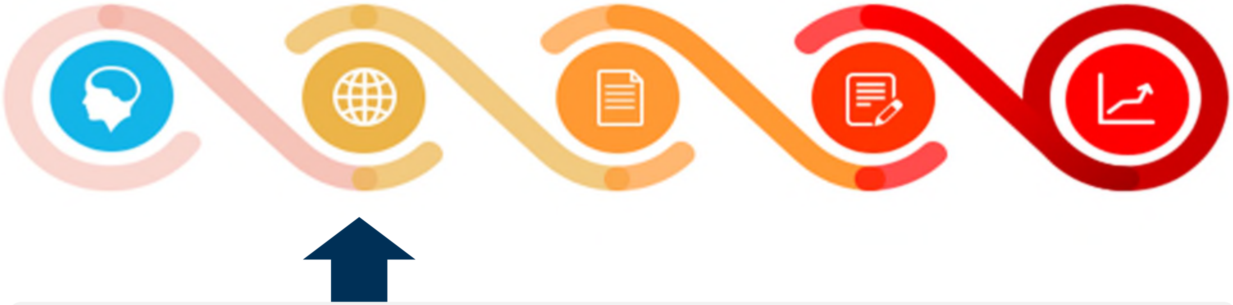
Moderate Risk

High Risk

"This company is **highly unlikely** to experience adverse impacts based on their level of exposure"

"This company is **somewhat likely** to have adverse impacts based on their level of exposure"

"This company is **highly likely** to have adverse impacts based on their level of exposure"



Kroll assesses a **low exposure risk** based on Kroll's review of the surface web and dark web exposure and data breach history associated with corporate emails and the digital footprint available at the time of the investigation.

Key Darkweb Data Findings

As of __________

SAMPLE OUTPUT

372 Marketplace listings appearing on **Genesis Market (44), Russian Market (122), Amigos Market (49) and 2Easy Shop (157)** containing **stolen credentials for websites stored in the victims' web browsers.** Records from the listings reference the **Targetco** domain **targetco.com.**

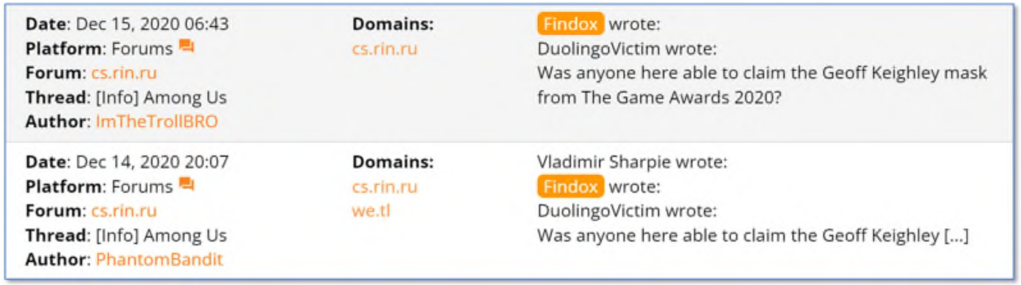
175 instances in which **Targetco** user credentials (username and password) appear within **information stealer malware logs.** The records pertain to end users who accessed the domains **targetco.com (173)** and **targetco.org(2).** The records include usernames and passwords in plain text.

443 Targetco corporate (@targeto.com) email addresses and password pairs were discovered within a variety of past third-party exposure incidents. The majority of exposures were from prior to 2020.

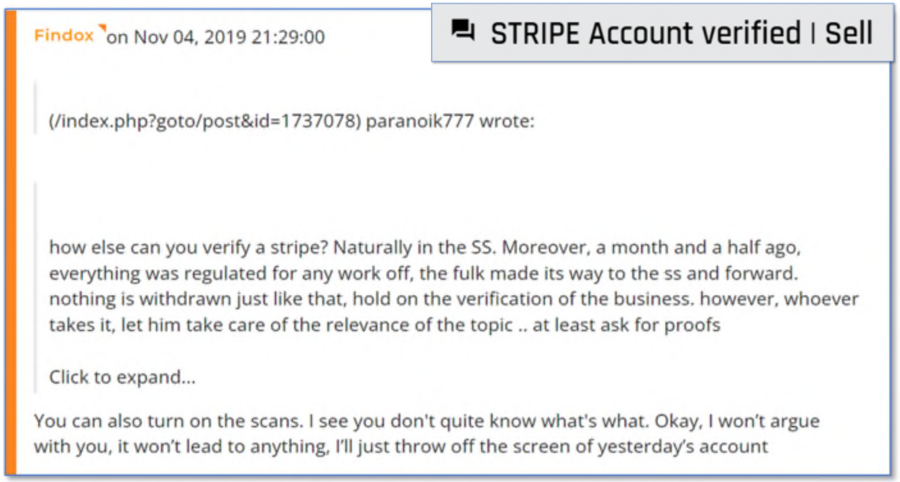
DDW Community Findings

"______"

- Kroll analysts identified **25** instances in which the term "_______" was mentioned in DDW Chat Forums and Boards since 2019.
- Mentions included DDW users by the same name posting in various forums regarding multiplayer video games and credit card accounts for verification.
- The authors and postings appear to be false positives for _______, Inc.



Date: Dec 15, 2020 06:43 **Platform**: Forums **Forum**: cs.rin.ru **Thread**: [Info] Among Us **Author**: ImTheTrollBRO	**Domains:** cs.rin.ru	Findox wrote: DuolingoVictim wrote: Was anyone here able to claim the Geoff Keighley mask from The Game Awards 2020?
Date: Dec 14, 2020 20:07 **Platform**: Forums **Forum**: cs.rin.ru **Thread**: [Info] Among Us **Author**: PhantomBandit	**Domains:** cs.rin.ru we.tl	Vladimir Sharpie wrote: Findox wrote: DuolingoVictim wrote: Was anyone here able to claim the Geoff Keighley [...]

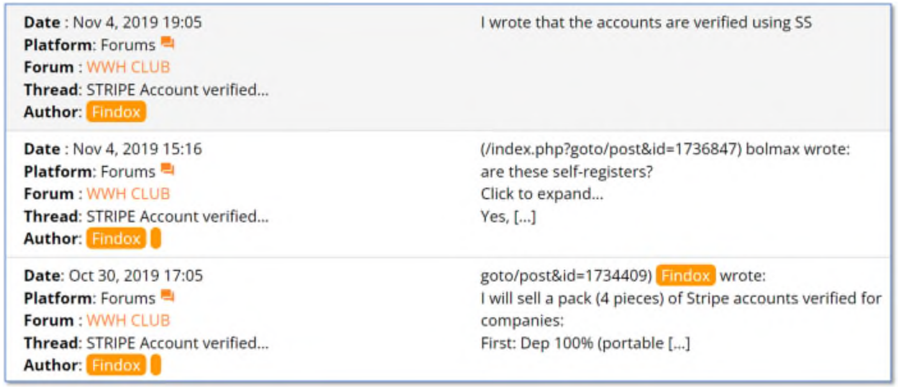


STRIPE Account verified I Sell

Findox on Nov 04, 2019 21:29:00

> (/index.php?goto/post&id=1737078) paranoik777 wrote:
>
> how else can you verify a stripe? Naturally in the SS. Moreover, a month and a half ago, everything was regulated for any work off, the fulk made its way to the ss and forward. nothing is withdrawn just like that, hold on the verification of the business. however, whoever takes it, let him take care of the relevance of the topic .. at least ask for proofs
>
> Click to expand...

You can also turn on the scans. I see you don't quite know what's what. Okay, I won't argue with you, it won't lead to anything, I'll just throw off the screen of yesterday's account



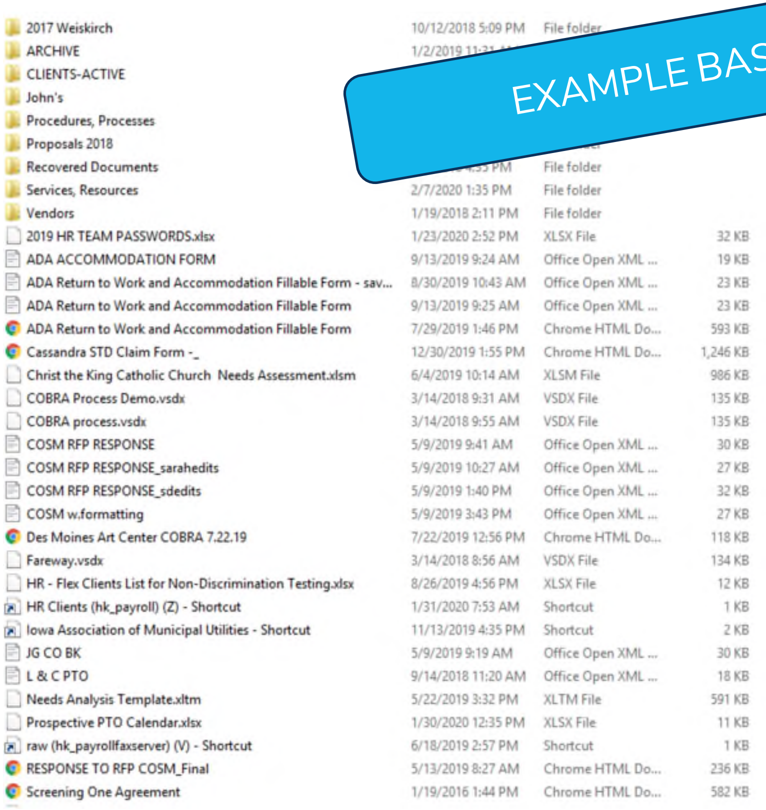
Date : Nov 4, 2019 19:05 **Platform**: Forums **Forum** : WWH CLUB **Thread**: STRIPE Account verified... **Author**: Findox	I wrote that the accounts are verified using SS
Date : Nov 4, 2019 15:16 **Platform**: Forums **Forum** : WWH CLUB **Thread**: STRIPE Account verified... **Author**: Findox	(/index.php?goto/post&id=1736847) bolmax wrote: are these self-registers? Click to expand... Yes, [...]
Date: Oct 30, 2019 17:05 **Platform**: Forums **Forum** : WWH CLUB **Thread**: STRIPE Account verified... **Author**: Findox	goto/post&id=1734409) Findox wrote: I will sell a pack (4 pieces) of Stripe accounts verified for companies: First: Dep 100% (portable [...]

Source: Flashpoint

Reference to Targetco domain on NetWalker Ransomware Blog from November 2020

- Kroll analysts discovered historical reporting of the ransomware-as-a-service (RaaS) operator, NetWalker, listing TARGET data on November 09, 2020.
- The data is no longer available on the Onion site provided in these screenshots, however DDW scraping tools log and maintain such records for review.

EXAMPLE BASE OUTPUT

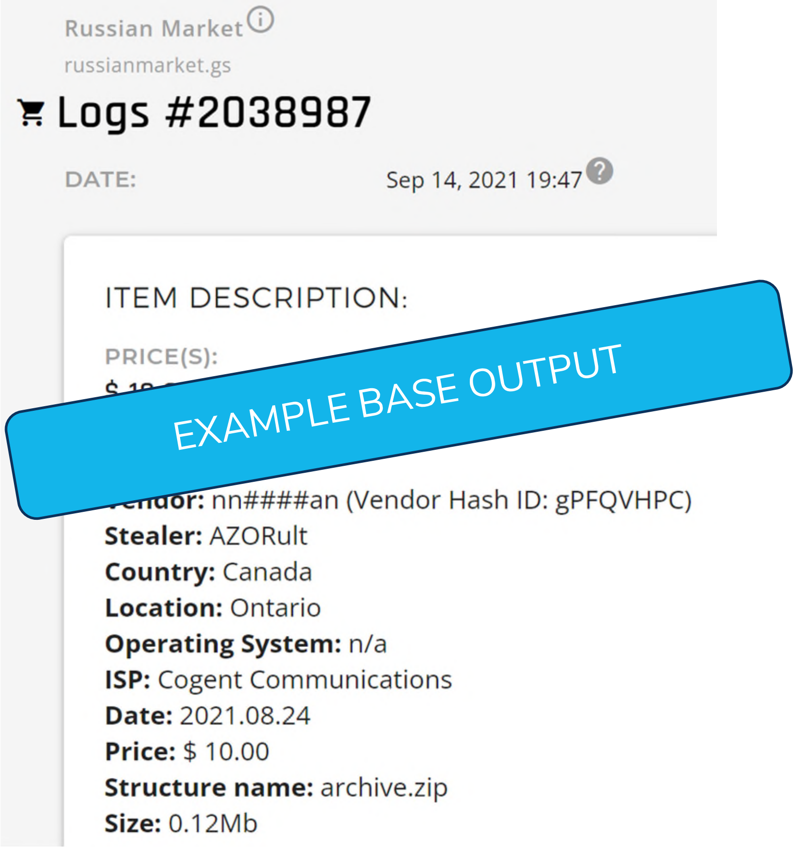


2017 Weiskirch	10/12/2018 5:09 PM	File folder	
ARCHIVE	1/2/2019 11:31 [illegible]	[illegible]	
CLIENTS-ACTIVE	[illegible]	[illegible]	
John's	[illegible]	[illegible]	
Procedures, Processes	[illegible]	[illegible]	
Proposals 2018	[illegible]	[illegible]	
Recovered Documents	[illegible] 4:35 PM	File folder	
Services, Resources	2/7/2020 1:35 PM	File folder	
Vendors	1/19/2018 2:11 PM	File folder	
2019 HR TEAM PASSWORDS.xlsx	1/23/2020 2:52 PM	XLSX File	32 KB
ADA ACCOMMODATION FORM	9/13/2019 9:24 AM	Office Open XML ...	19 KB
ADA Return to Work and Accommodation Fillable Form - sav...	8/30/2019 10:43 AM	Office Open XML ...	23 KB
ADA Return to Work and Accommodation Fillable Form	9/13/2019 9:25 AM	Office Open XML ...	23 KB
ADA Return to Work and Accommodation Fillable Form	7/29/2019 1:46 PM	Chrome HTML Do...	593 KB
Cassandra STD Claim Form -_	12/30/2019 1:55 PM	Chrome HTML Do...	1,246 KB
Christ the King Catholic Church Needs Assessment.xlsm	6/4/2019 10:14 AM	XLSM File	986 KB
COBRA Process Demo.vsdx	3/14/2018 9:31 AM	VSDX File	135 KB
COBRA process.vsdx	3/14/2018 9:55 AM	VSDX File	135 KB
COSM RFP RESPONSE	5/9/2019 9:41 AM	Office Open XML ...	30 KB
COSM RFP RESPONSE_sarahedits	5/9/2019 10:27 AM	Office Open XML ...	27 KB
COSM RFP RESPONSE_sdedits	5/9/2019 1:40 PM	Office Open XML ...	32 KB
COSM w.formatting	5/9/2019 3:43 PM	Office Open XML ...	27 KB
Des Moines Art Center COBRA 7.22.19	7/22/2019 12:56 PM	Chrome HTML Do...	118 KB
Fareway.vsdx	3/14/2018 8:56 AM	VSDX File	134 KB
HR - Flex Clients List for Non-Discrimination Testing.xlsx	8/26/2019 4:56 PM	XLSX File	12 KB
HR Clients (hk_payroll) (Z) - Shortcut	1/31/2020 7:53 AM	Shortcut	1 KB
Iowa Association of Municipal Utilities - Shortcut	11/13/2019 4:35 PM	Shortcut	2 KB
JG CO BK	5/9/2019 9:19 AM	Office Open XML ...	30 KB
L & C PTO	9/14/2018 11:20 AM	Office Open XML ...	18 KB
Needs Analysis Template.xltm	5/22/2019 3:32 PM	XLTM File	591 KB
Prospective PTO Calendar.xlsx	1/30/2020 12:35 PM	XLSX File	11 KB
raw (hk_payrollfaxserver) (V) - Shortcut	6/18/2019 2:57 PM	Shortcut	1 KB
RESPONSE TO RFP COSM_Final	5/13/2019 8:27 AM	Chrome HTML Do...	236 KB
Screening One Agreement	1/19/2016 1:44 PM	Chrome HTML Do...	582 KB

DDW Marketplaces - Infostealer Malware

DDW Findings

- Kroll identified marketplace listings on **Genesis Market (44), Russian Market (122), Amigos Market (49) and 2Easy Shop (157)** containing **stolen credentials for various websites which were stored in the victims' web browsers. 372** total records from the listings reference the **Targetco.** domain **[targetco].com.**
- The records were stolen as a result of a browser compromise affecting the victims.
- The victims are infected with Information stealer malware, also referred to as "infostealers," developed with capabilities that allow them to infect victim devices and collect a variety of data types, including files, virtual private network ("VPN") session information, browser histories, fingerprints, login credentials, and financial data.
- Common infostealer variants include Vidar, Taurus, Racoon, AZORult, and RedLine.
- The records for sale likely pertain to **Targetco.** customers/users, as opposed to employees.



Russian Market ⓘ
russianmarket.gs

Logs #2038987

DATE: Sep 14, 2021 19:47

ITEM DESCRIPTION:

PRICE(S):
$ 1

EXAMPLE BASE OUTPUT

Vendor: nn####an (Vendor Hash ID: gPFQVHPC)
Stealer: AZORult
Country: Canada
Location: Ontario
Operating System: n/a
ISP: Cogent Communications
Date: 2021.08.24
Price: $ 10.00
Structure name: archive.zip
Size: 0.12Mb

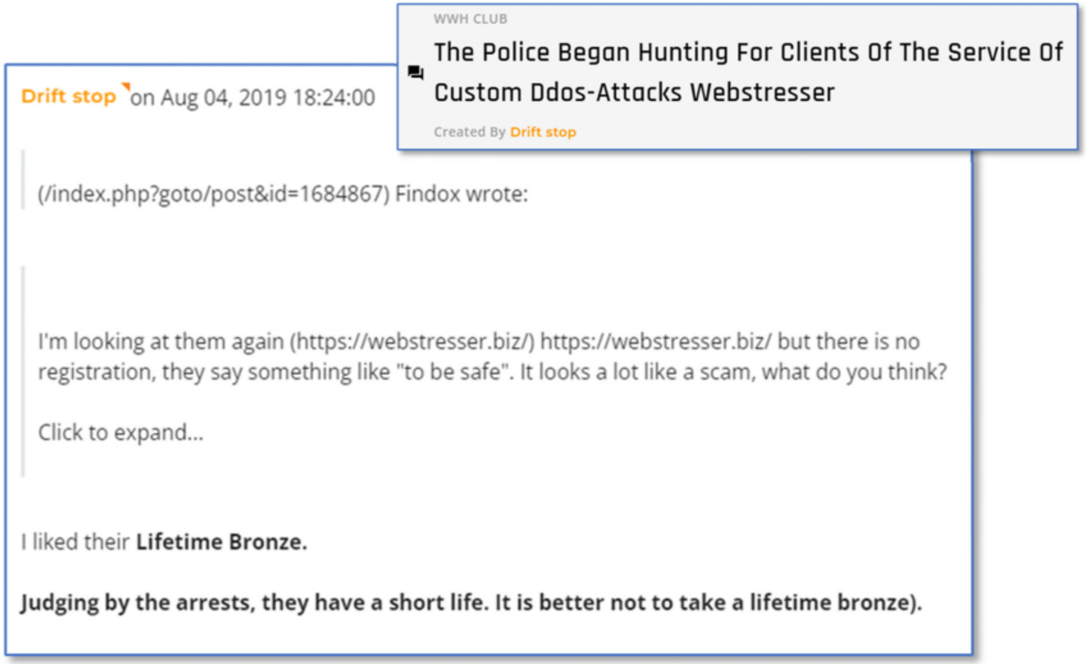
Mozilla Firefox Login: + Password: + Cookie: -

[redacted]

DDW Community Findings

"______" + ("Core" | "FDA" | "ESGx" | "ESG" | "ESMA" | "SFDR" | "TCFD" | "Debtdomain" | "Data")

- Kroll analysts identified **8** instances in which the term "**______**" was mentioned along one or more of the abovementioned key terms in DDW Chat Forums and Boards since 2019.
- Many of the results overlap with the results for the key term "______" provided on the previous slide. Additional results were also related to users with the name ______ and unrelated to ______, Inc.



WWH CLUB

The Police Began Hunting For Clients Of The Service Of Custom Ddos-Attacks Webstresser

Created By Drift stop

Drift stop on Aug 04, 2019 18:24:00

(/index.php?goto/post&id=1684867) Findox wrote:

I'm looking at them again (https://webstresser.biz/) https://webstresser.biz/ but there is no registration, they say something like "to be safe". It looks a lot like a scam, what do you think?

Click to expand...

I liked their **Lifetime Bronze.**

Judging by the arrests, they have a short life. It is better not to take a lifetime bronze).

Source: Flashpoint

Thank You

For more information, please contact:

Ira Levy
Associate Managing Director
Kroll Cyber Risk – Advisory Services

555 12th Street NW
Suite 600
Washington, DC 20004

Mobile: +1 443 250 9549
ira.levy@kroll.com

John deCraen
Associate Managing Director
Kroll Cyber Risk – Advisory Services

1700 Pacific Avenue
Suite 1600
Dallas, TX 75201

Mobile: +1 (817) 881-8879
john.decraen@kroll.com

About Kroll

As the leading independent provider of risk and financial advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's team of more than 6,500 professionals worldwide continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at www.kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.