IT & Cyber Due Diligence

2025 Insights for PE Firms & Portfolio Companies

March 26, 2025

forvis mazars

Agenda

- Introductions
- Learning Objectives
- High-Level Overview of IT/Cyber Diligence
- Key Considerations around AI & Cybersecurity in 2025
- Investment in IT/Cyber Projects
- Q&A

Presenters

Tyler Leach

Director | Transaction Advisory

tyler.leach@us.forvismazars.com

919.875.4973

Andrea Tomczak

Manager | Transaction Advisory

andrea.tomczak@us.forvismazars.com

872.285.7222

Learning Objectives

By the end of this session, you will be able to:

Identify what IT/Cyber Due Diligence is & why it's important to consider during buy- & sell-side transactions.

Discuss key considerations in 2025 around AI & Cybersecurity that Companies are facing in the IT/cyber landscape.

Recognize why companies should invest in IT/cyber project recommendations during the hold period.

forvis mazars

High-Level Overview

IT/Cyber Due Diligence
Breakdown

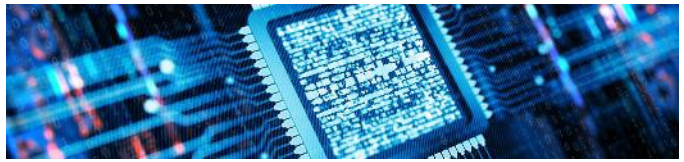
What is IT/Cyber Due Diligence?

- **IT & Cyber Due Diligence** is an evaluation of a company's Information Technology & cybersecurity measures, typically carried out during mergers or acquisitions, to identify potential risks & vulnerabilities associated with data security & system operations. The process involves an analysis of the company's IT environment to uncover potential cybersecurity threats & weaknesses that could impact the acquiring entity. Essentially, it's an investigation into the company's technological landscape to assist buyers with a secure & seamless integration.
- IT & Cyber Due Diligence involves assessing the following key areas:

IT Governance

Application Software

IT Security



IT Infrastructure & Operations

Data Privacy

HIPAA (as applicable)

IT/Cyber Due Diligence
Select Industries

- Construction
- Manufacturing & Distribution
- Government Contracting
- Professional Services
- Financial Services
- Retail
- Healthcare & Life Sciences
- Software & Technology

Key Considerations in 2025

What Is Artificial Intelligence (AI)?
Industry Overview

Technology capable of performing functions normally associated with human intelligence such as reasoning, learning, & self-improvement

- Machine Learning
- Natural Language Processing
- Predicative Analytics
- Robotics

Benefits

- Increased speed & productivity
- Ability to quickly generate cognitive insights from large data sets
- Always available to engage

Use Cases

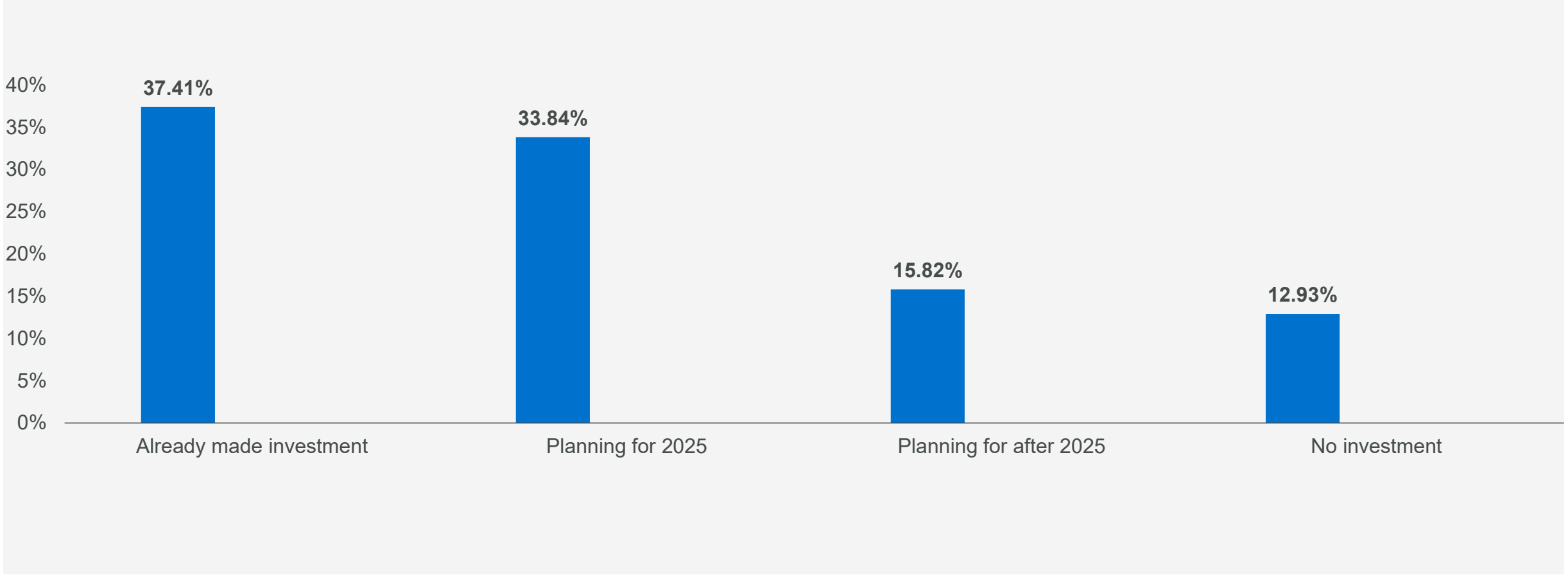
- Improve features & functionality of products & services
- Optimize & enhance business processes
- Prevent/detect fraud & cybersecurity incidents

Examples

- Customer service
- Fraud detection
- Sales & marketing

Organizations' Investment Into Generative AI
Understanding Where AI Technology Is Being Adopted & Invested In

InfoTech's Future of IT 2025 Survey



Source: InfoTech's Future of IT 2025 Survey, 2024; *n*=588

Key AI Considerations

Key Considerations

- **Algorithmic bias** could result in poor business decisions &/or negatively impact customers or society at large
- There is a **lack of trust in adoption** of AI because the company is unable to explain & demonstrate how AI systems reach conclusions or generate output
- Trust in the information … lack of adoption
- **Inaccurate data/models**
- Loss allowances or impairments inaccuracies
- **Cybersecurity compromised** based on AI development technology
- AI could generate **inaccurate or harmful content,** which could result in loss of customer trust or negative publicity
- The risk of using **not fully vetted AI data** to present/publish research
- The use of personally identifiable information (PII) data to train AI systems could result in violations of privacy laws & regulations
- **Regulatory fines**

forvis mazars

AI Governance

Governance Framework

- Utilizing a framework to review, **manage AI initiatives responsibly**, **enable compliance** with laws, & **align AI usage** with self-defined ethical standards
- Effective AI governance **balances innovation with risk management & safeguards** against unintended consequences

Policies

- **Develop** internal **policies** that define clear **roles & responsibilities** for AI initiatives
- Establish & **integrate ethical guidelines & principles** into AI development processes
- Transparency, accountability, & **bias mitigation** are important considerations for AI governance

Oversight

- Establish committees to oversee AI projects to ensure compliance (internal & regulatory compliance)
- Implement regular audits & continuous monitoring processes to assess AI
- Establish **oversight of third-party** AI Systems

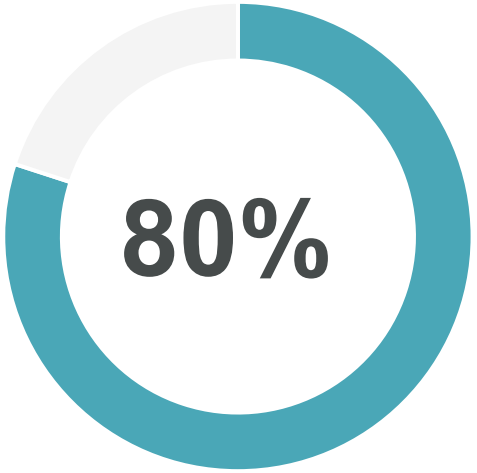
AI FRAMEWORKS & PRINCIPLES

European Union AI Act | IEEE Global Initiative on Ethics of Autonomous & Intelligent Systems | White House Executive Order on AI
ISO 42001 | NIST AI RMF | OECD AI Principles | OWASP AI Security & Privacy Guide | Virginia Consumer Data Protection Act (CDPA)

Cybersecurity Incident Trends
Data Breaches & Cyberattacks

$4.88 million

- According to an annual study by IBM & Ponemon Institute, the global **average data breach cost** in 2024 was **$4.88 million**, a 10% increase from 2023.



- A Harvard Business Review noted in 2023 that **80%** of cyberattacks are **due to human error.**

•Sources: “Cost of a Data Breach Report 2024,” ibm.com.
•“Human Error Drives Most Cyber Incidents. Could AI Help?,” hbr.org, May 3, 2023.

forvis mazars

FBI’s IC3 Five-Year Statistics

3.79 Million
Total Complaints

$37.4 Billion
Total Losses

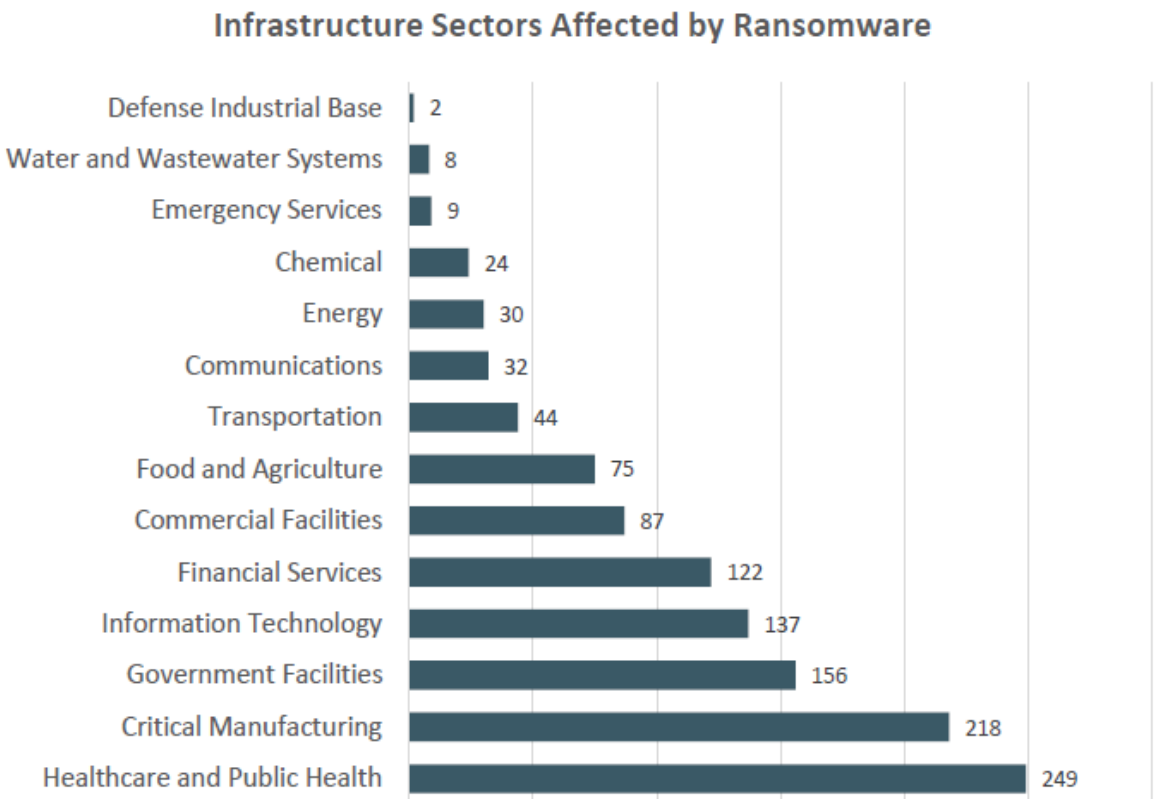
Source: FBI’s Internet Crime Compliant Center 2023 Report

Ransomware

For 2023, the FBI's Internet Crime Complaint Center (IC3) received **2,825 complaints** identified as ransomware with adjusted losses of more than **$59.6 million**.

Ransomware is a type of malicious software, or malware, that encrypts data on a computer, making it unusable. In addition to encrypting the network, the cybercriminal will often steal data off the system & hold that data hostage until the ransom is paid. If the ransom is not paid, the entity's data remains unavailable.

The IC3 received **1,193 complaints** from organizations belonging to a critical infrastructure sector that were affected by a ransomware attack. Of the 16 critical infrastructure sectors, IC3 reporting indicated 14 sectors had at least one member that fell to a ransomware attack in 2023.



Source: FBI's Internet Crime Compliant Center 2023 Report

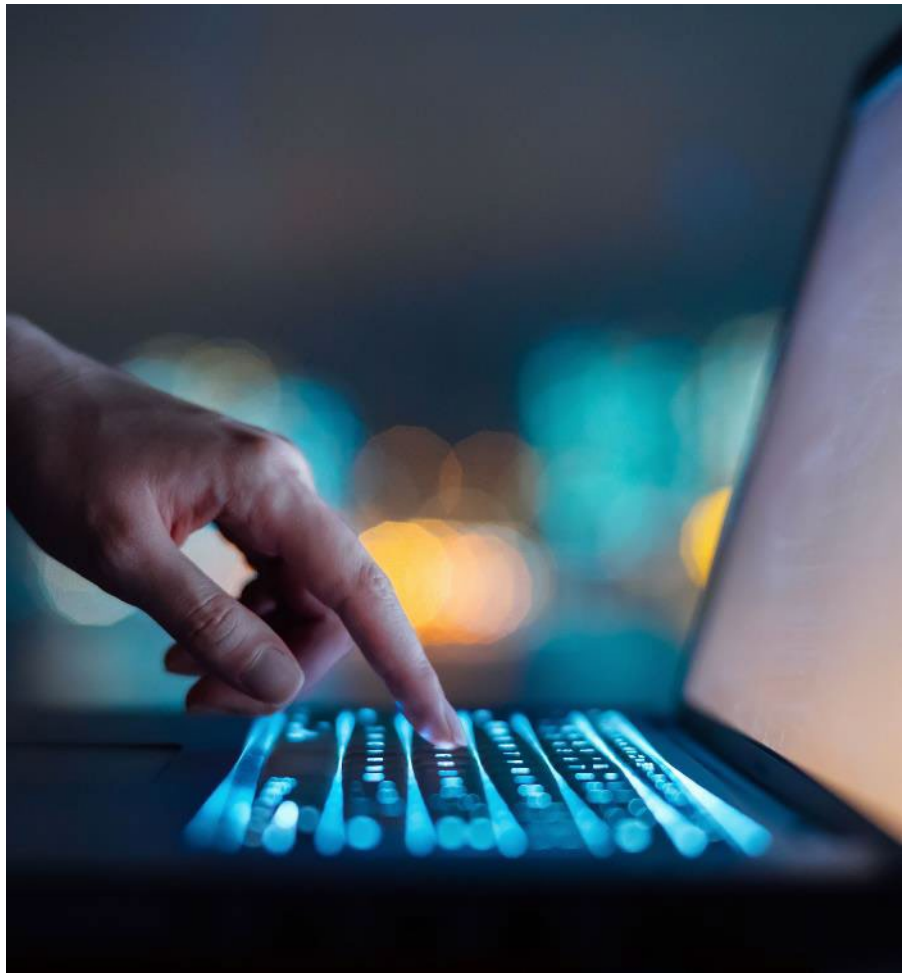
forvis mazars

Business Email Compromise

In 2023, the IC3 received **21,489 complaints** of Business Email Compromise (BEC)/Email Account Compromise (EAC) complaints with adjusted losses at nearly **$2.9 billion**.

IC3 Recovery Asset Team (RAT) Guidance – Est. February 2018

- Contact the originating financial institution as soon as fraud is recognized to request a recall or reversal & a Hold Harmless Letter or Letter of Indemnity.
- File a detailed complaint with www.ic3.gov. It is vital the complaint contain all required data in provided fields, including banking information.
- Visit www.ic3.gov for updated PSAs regarding BEC trends as well as other fraud schemes targeting specific populations, like trends targeting real estate, pre-paid cards, & W-2s, for example.
- Never make any payment changes without verifying the change with the intended recipient; verify email addresses are accurate when checking email on a cell phone or other mobile device.



Source: FBI's Internet Crime Compliant Center 2023 Report

forvis mazars

Key Cybersecurity Considerations

IT Governance

- Maintain a strong **information security program**
- Maintain a strong **incident response program**
- Ensure **business continuity/DR & vendor management** policies & procedures address cybersecurity
- Ensure **cybersecurity awareness training** is performed regularly (educate & motivate)
- Join an **information sharing & analysis center (ISAC)** or other information sharing

Application Software & Infrastructure & Operations

- Enforce **application whitelisting** controls & **remove** unauthorized applications
- Track, report, independently test, & update security **patches** based on a risk priority schedule (Microsoft & non-Microsoft patches)
- Maintain accurate **asset inventories** for hardware & software, including **data classification**
- **Segment** internal networks to isolate critical systems
- **Air gap** your backups to keep them out of reach of an attack
- Make your air-gapped backups **immutable**

forvis mazars

Key Cybersecurity Considerations

IT Security

- Consider how **cybersecurity insurance** should fit into your risk management program
- Use **multifactor** or **two-factor** for O365, VPN, remote sessions, & privileged access
- **Remove local administrator** rights to reduce malicious software installs
- **Tune existing security tools** – web content, email filtering, end point, etc.
- Deploy **cloud-based security** software & end-point protection, *e.g.*, SentinelOne, Crowdstrike, Windows Defender, etc.
- Use **security information & event management (SIEM)** tools with “defense in depth” approach
- **Change your passwords** more frequently during this time
- Be aware of **insider threat** – layoffs, disgruntled, etc. Think zero trust!
- Perform **frequent cyber risk assessments**, penetration tests, vulnerability assessments, & IT control audits

Data Privacy / HIPAA

- Implement strong cloud-based **data loss prevention** controls
- Ensure **data encryption** is enforced to protect confidential data

forvis mazars

Ransomware: Key Questions for Leaders to Ask

What to Do If It Happens to You?

Incident Response Plan: IT & Cybersecurity staff must develop, test, & execute a **company-centric IRP**.

Verify Backups: Check the **integrity of your backups** & ensure they are not compromised. Use them to restore your data if possible.

Contact Law Enforcement: Report the ransomware attack to **authorities & cybersecurity agencies.**

Cybersecurity Experts: Engage with **professional incident response teams** to assess the situation & explore recovery options.

Proof of Life: Ask the threat actors for copies of files that have been encrypted as **proof they can be decrypted**.

Cybersecurity Insurance Coverage: Consider acquiring cybersecurity insurance if you handle sensitive information or your business relies heavily on digital operations.

forvis mazars

Investment in IT/Cyber Projects

Reducing Tech Debt
Identify, Measure, & Manage

- Technical debt refers to suboptimal technology infrastructure that accumulates over time that can significantly impact a company's profitability, operational efficiency, & overall growth trajectory.
- Technical debt is often likened to a "tax" a company pays for the work required to upgrade, replace, & eliminate redundant & obsolete technology. It can hold a company back, dragging it down into inefficiency & stagnation.

Examples of Tech Debt:

- Messy code is deployed to meet a deadline.
- Equipment refreshes are deferred.
- Security vulnerabilities are left unpatched.
- Machine learning algorithms are not analyzed for accuracy or bias.
- Data is ungoverned; APIs don't follow standards.
- Broken service management processes are not fixed.
- Training budgets are cut.
- Old technologies are not replaced.
- Redundant systems.

Source: Info Tech Research Group

forvis mazars

Reducing Technical Debt
Investment in IT/Cyber Projects

Importance of Investing in IT/Cyber Projects

- **Strengthen Competitive Position:** Organizations that manage their technical debt effectively are better positioned to adapt to market changes, deliver greater customer experiences, remain competitive, & attract future buyers.
- **Enhance Operational Efficiency:** Reducing technical debt minimizes system inefficiencies & maintenance burdens, allowing teams to focus on innovation & value-added activities.
- **Improve Product Quality:** Addressing technical debt leads to fewer bugs & faster implementation of new features, resulting in higher-quality products & services.
- **Maintain Employee Retention:** A well-maintained IT environment reduces frustration among teams, leading to higher job satisfaction & retention rates.
- **Mitigate Risks:** Proactively managing technical debt helps identify & mitigate hidden risks, preventing costly disruptions & ensuring smoother operations.
- **Measure Resources:** As technical debt reduces, it is likely employees can reallocate time & priorities to align with the business. Leadership will likely have access to additional information to make informed decisions.

Source: Info Tech Research Group

IT/Cyber Due Diligence
Post-Close Offerings

- IT Current-State Assessments (preparing for future sale)
- IT Organizational Assessments
- IT Policy Creation
- IT Budget/Spend Analysis
- Cloud Security Alliance (CSA) Cloud – Controls Matrix (CCM)
- Government Contracting & Cybersecurity Maturity Model Certification (CMMC) Compliance
- ISO 27001 Solutions
- Information Technology & Cybersecurity Audits
- Payment Card Industry (PCI) Compliance
- SOX & IT General Controls Testing

Working cross-functionally with our **Private Equity Value Creation Team**

+

Business Technology Solutions Teams

forvis mazars

IT/Cyber Due Diligence
Post-Close Offerings

- Data Privacy & Compliance: Policy & Procedure Development, Data Privacy Impact Assessments (DPIA), Record of Processing Activity (ROPA) Documentation, Internal Audit Support, California Consumer Privacy (CCPA/CPRA), Global Data Protection Regulation (GDPR), NIST Privacy Framework, State Data Breach Notification Rules
- Ransomware Risk Assessments & Simulations
- Penetration Testing
- Overwatch – Forvis Mazars 24/7 Managed Security Services
- Business Continuity Planning
- Cybersecurity Awareness Training
- Incident Response Plan Development & Training Services
- Third-Party Risk & Vendor Management
- Virtual Chief Information Security Officer (vCISO) Advisor Services

Working cross-functionally with our **Private Equity Value Creation Team**

+

Business Technology Solutions Teams

forvis mazars

Questions?

forvis mazars

Contact

Forvis Mazars

Tyler Leach
Director
P: 919.875.4973
tyler.leach@us.forvismazars.com

Andrea Tomczak
Manager
P: 810.624.9066
andrea.tomczak@us.forvismazars.com

forvis mazars