Enhancing Resilience
in Online Gaming:

Navigating Cybersecurity, Privacy, and Insurance

APRIL 16, 2025

With You Today

JONATHAN COLOGNESI

Assurance Principal

jcolognesi@bdo.com

MARK MELNYCHENKO

Privacy Technology Practice Leader

mmelnychenko@bdo.com

MATT HANSON

Forensics Managing Director

mhanson@bdo.com

WAYNE ANDERSON

Cyber, Data Security and Privacy Director

wanderson@bdo.com

Learning Objectives

01

Understand the impact of recent cybersecurity incidents and regulatory actions on the online gaming industry.

02

Explore the evolving role of cyber insurance and its implications for gaming companies.

03

Gain insights into enhancing privacy and cybersecurity measures to support organizational resilience.

Our Agenda Today

State of the Industry

Cyber Risk, Response and Recovery for the Gaming Industry

Forensic Insights: Elevating Privacy in Online Gaming and Digital Profiles

Cybersecurity State of Threat

Panel Discussion

State of the Industry

Jonathan Colognesi

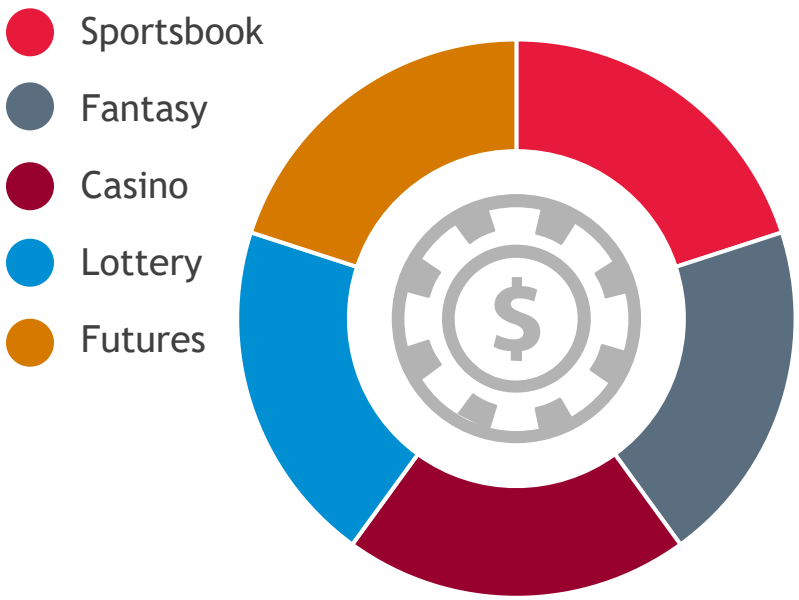
ONLINE GAMING

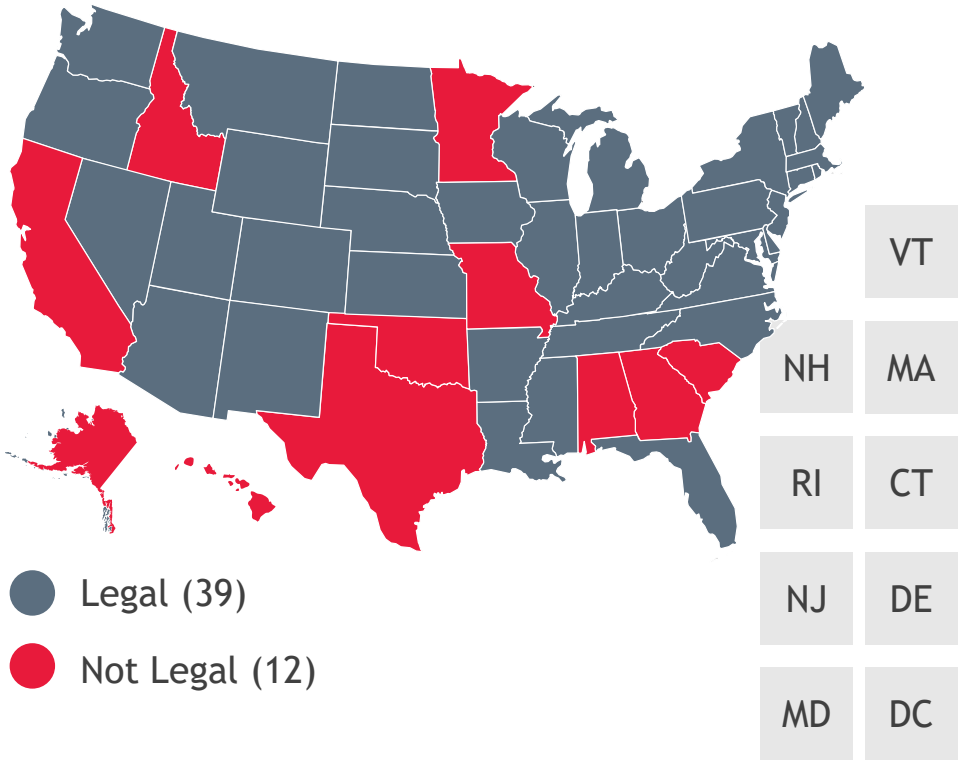
Evolving Industry

User Growth Drivers

- Continued Product Innovation
- Regulatory Acceptance
- Growing User Adoption
- Evolving User Demographics

Online Gaming Segments



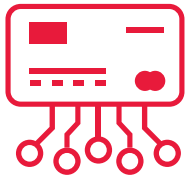


Cyber Risk, Response and Recovery for the Gaming Industry

Matt Hanson

PROTECTING AGAINST RISK

What makes the online gaming industry a hacker's target?



Customer, payment info

Targeted campaigns

Key asset is customer confidence

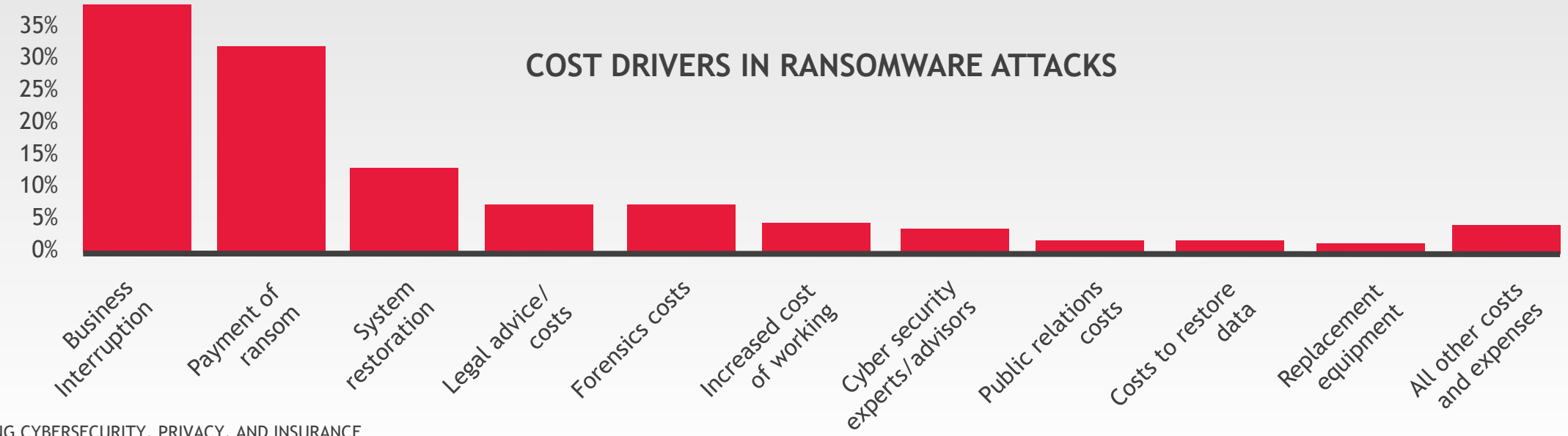
Interdependent systems / many entry points

Every hour counts

High stakes events

Cost of Ransomware Crisis

2015	2017	2021	2024	2026	2028	2031
$325M	$5B	$20B	$42B	$71.5B	$157B	$265B



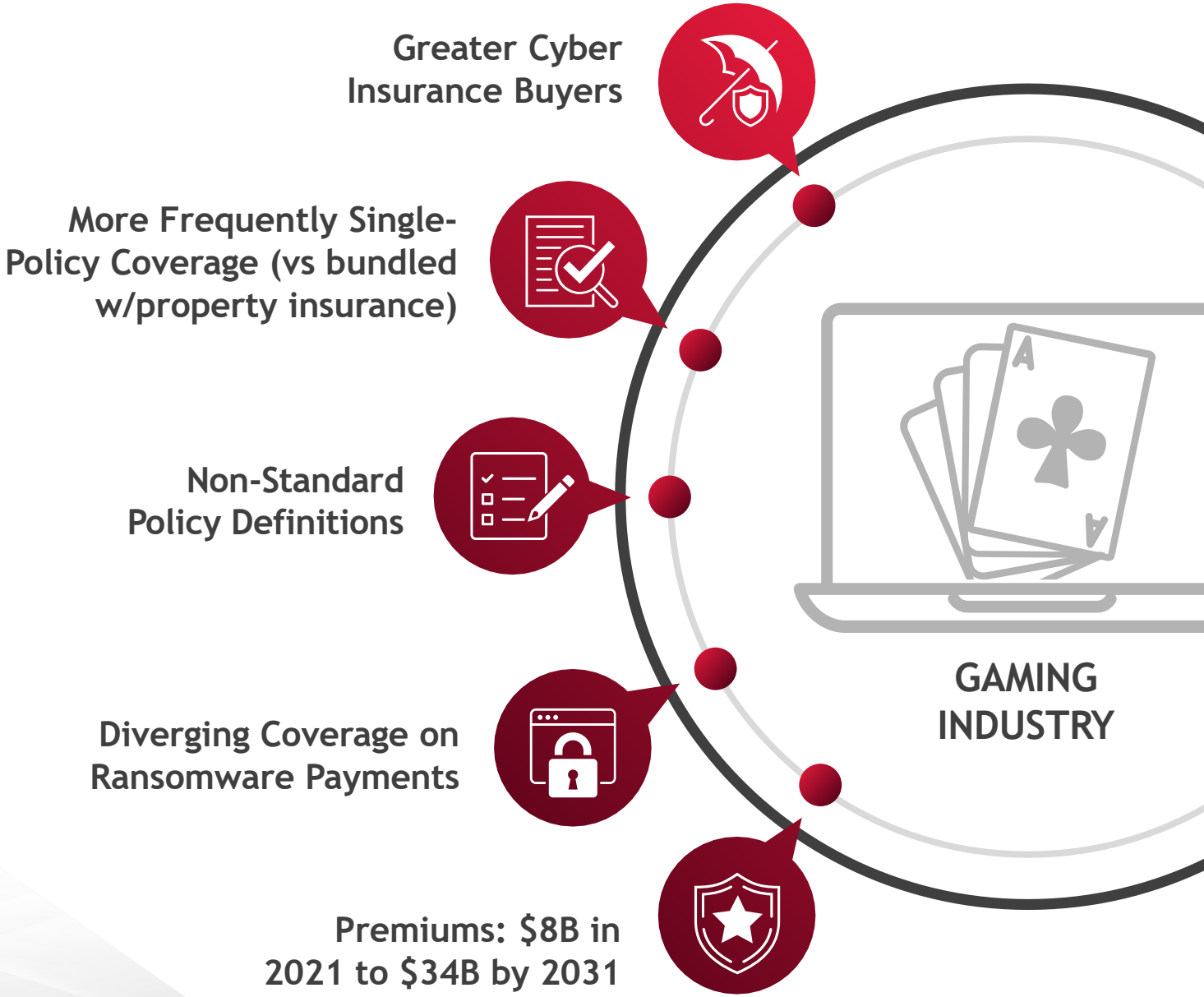
*Cyber Security Ventures Global Report

Cyber Insurance Trends

What is changing in cyber insurance?

- Greater proportion of insurance buyers include cyber coverage
- Increase in single-policy written by cyber insurer, which helps definitions
- Policy language is not uniform
- Ransomware is driving claim costs
- Rates increasing

Source: Cyber Security Ventures



Cyber Insurance Policies

KEY PROVISIONS

- Retention (Deductible) - dollar amount and waiting period
- Aggregate Limit of Liability
- Limits per subcategory of coverage (examples):
  - Privacy and Security Liability
  - PCI DSS Assessments
  - Cyber Extortion
  - Business Income Loss
  - Reputational Harm
  - Claim Preparation Costs
- Dependent Business Income Loss including IT and non-IT providers

Every policy is different; review with your insurance broker/legal advisors

What makes these claims different?

- Number of locations/revenue streams all impacted at once — **often the entire organization**
- Contemporaneous documentation is critical
- Timeline and narrative development is important — when did systems come back online and how long did it take to work through backlog
- Use of market data in analyses is particularly useful
- Use of employees and IT labor
- Waiting period analysis
- Reliability of financials
- Evolving threat landscape and challenges

Claims Handling Best Practices

- Maintaining contemporaneous documentation is critical
- Establish a general ledger code to record extraordinary expenses
- Insurance companies have “panels” of vendors for services like legal, computer forensics, ransom negotiations, etc. Make sure you know who you can hire and beware!
- Understanding insurance company(s) requirement for a reserve
- Developing a timeline and narrative of your losses
- You prepare your claim, rather than letting the insurance company prepare it
- Remediation and concept of upgrade

Forensic Insights: Elevating Privacy in Online Gaming and Digital Profiles

Mark Melnychenko

Current State of Privacy Laws

The General Data Protection Regulation (GDPR) was the first major "comprehensive" privacy law passed, which applies to residents of the European Union (EU) and went into effect in 2018. It gives individuals rights over their personal information and enacts requirements for companies which collect and process it.

Since then, many similar laws have been passed around the globe. In the United States (US), there is no comprehensive federal law. However, 19 states have passed their own thus far with California leading the way and 13 state laws in effect as of January 2025.

Remaining compliant with all these laws can be daunting. Some of the challenges include:

- **Jurisdictions:** Whether a given law applies is based on the jurisdiction where the data subjects live, not on where a company is located. For example, if you collect and process data from people who live in the EU, then you need to consider the GDPR.
- **Volatility:** New laws are being passed frequently, and existing laws are sometimes updated, making it difficult to keep up with the changing legal landscape. For example, 13 US state laws went into effect within 4 years and California already released updates to its original law.
- **Overlaps:** In some jurisdictions, there are federal laws which may overlap with more regional laws. For example, Canada has a federal privacy law called the Personal Information Protection and Electronic Documents Act (PIPEDA), but some of its provinces have also passed their own.

Types of Personal Information

Most modern privacy laws define "personal information" broadly to include any element of data associated with an identified or identifiable individual. Companies in the Gaming & Leisure space potentially collect and use many types of personal information:

- Contact information
- Customer profile data and pictures
- Reservation details
- Loyalty program data
- Transaction records for hotel stays, gaming transactions, etc.
- Government ID records
- Demographic data
- Online usage history
- Financial and tax-related data
- Social media account linkages
- Biometric data
- Employee and vendor data

It is crucial that this data be well protected and that requirements within applicable privacy laws are understood, to ensure a compliant privacy program.

Privacy Incident Handling

Privacy incidents generally refer to cases where someone's personal information has been mishandled. Some privacy incidents are caused by security incidents while others are not. Common types include:

- Breaches
- Unauthorized or Unintentional Disclosure
- Data Loss or Improper Disposal
- Lack of Encryption

When a privacy incident occurs, the process for handling it should include the following steps:

Immediate Response
Identify nature and scope of incident; contain to prevent further issues

Assessment
Evaluate impact to affected individuals and the organization; identify related risks

Notifications
Inform relevant internal stakeholders; inform affected individuals and regulatory authorities per legal requirements

Investigation & Remediation
Identify and document root cause of the incident; fix issues as needed; update policies and procedures as needed

Recover
Restore lost or compromised data as needed; ensure affected systems are restored to normal operation

Monitoring & Reporting
Implement ongoing monitoring as needed to ensure effectiveness of remediation; report on incident as needed per regulatory requirements

Cybersecurity: State of Threat

Wayne Anderson

Breach Response

A LONG AND INTENSIVE PROCESS

277

Average number of days needed to identify and contain a cybersecurity breach (IBM)

The New Trend

48 Hours

From initial breach to
deployment of Ransomware

Initial Compromise

The Adversary

WHO THEY ARE

Nation States

Motive: Geopolitical Influence and Espionage

Targets: Organizations of strategic interest

Methods: Custom intrusion tools, zero-day exploits

Ecrime

Motive: Profit

Targets: Various industries

Methods: Ransomware, banking trojans, commodity malware

Hacktivists

Motive: Social/Geopolitical causes

Targets: Various industries

Methods: Defacement, DDoS

Insider Threats

Motive: Profit and satisfying discontent, unsuspecting users or compromised user devices

Targets: Organizations

Methods: Data Theft or initial access

Different Motives Drive Different Threat Actors

Notable Attacks

Casino

Target: MGM Resorts – experienced widespread system outages and service disruptions in its properties due to a cyberattack.

Caesars Entertainment - similarly to MGM, reported a data breach where many of its loyalty program members' personal information was accessed, and services disrupted.

Impact: MGM customers faced issues like sporadic keycard problems in the hotels, non-functioning slot machines, out-of-order ATMs, and troubles cashing out their winnings.

After the Caesars breach was revealed, it was reported that Caesars paid around half of the $30 million the attackers demanded to ensure the non-release of the stolen customer data.

Adversary/Malware Families: A ransomware group named Alphv, (a.k.a. BlackCat) based in Russia, claimed responsibility for the attack on MGM. This group denied involvement in the Caesars attack.

Supply Chain - Software

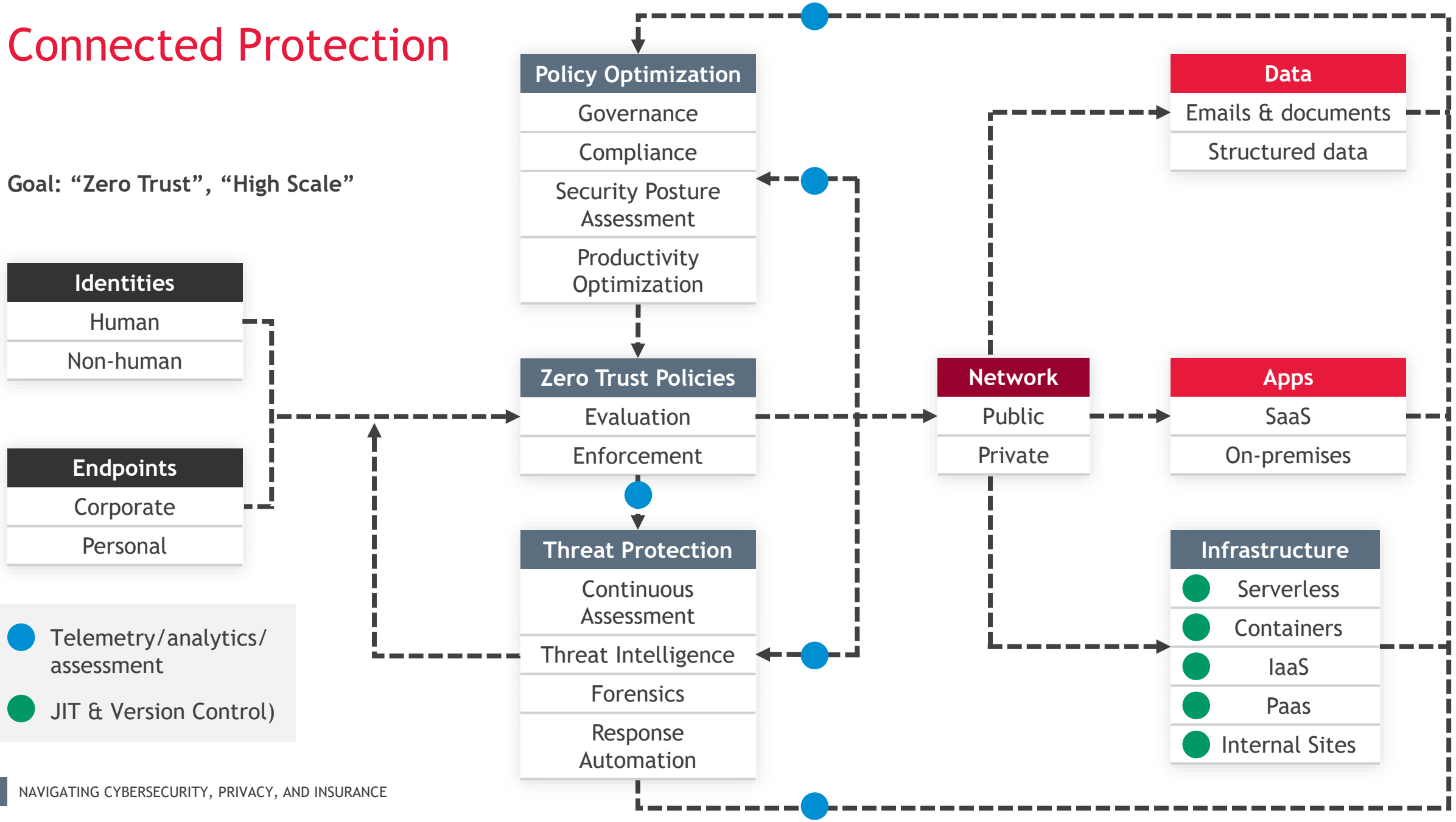
Target: Progress Software – experienced a supply chain attack on its popular MoveIT platform, which led to a compromise of clients using the MoveIT software.

Impact: Organizations globally were impacted, by the vulnerability in this file transfer application which allowed adversaries to gain access to confidential files of over 600 organizations, impacting over 40 million people. The objective was to exfiltrate data and coerce organizations into ransom payments to prevent the data from being shared publicly.

Adversary/Malware Families: Cl0p ransomware family is known for its "double extortion" tactics, where they steal and encrypt data, then threaten to publish the stolen data if the ransom isn't paid.

Connected Protection

Goal: “Zero Trust”, “High Scale”



Use Artificial Intelligence to Enhance Cybersecurity

Cybersecurity operates at hyper-speed protecting many platforms and assets. Artificial intelligence tracks signals beyond human speed and aids responders in making effective real time mitigations.

On average, organizations now utilize **147** public cloud services spanning SaaS, PaaS, and IaaS. (1)

66% of organizations have developed an AI strategy, with **36%** already implementing it. (2)

Capabilities	Strategic Benefit
Generative AI for Security Operations Analysts	Speed response and reduce the burden of investigation. Close cybersecurity skills gap. **Example:** Copilot for Security from Microsoft
AI enhanced detection and response	Analyze high volume signals to find "true threats" and close gaps quickly. **Example:** Microsoft Sentinel, Google Chronicle, Palo Alto Prisma
Machine Learning enhanced data security	Identify sensitive information with non-standard formats like contracts, invoices, and resumes to meet regulatory and security obligations. **Example:** Microsoft Purview, Microsoft Insider Risk Management, BigID
AI-aided governance and risk platforms	Reduce burden of governance assessments. Use Natural Language capabilities to interpret and categorize capabilities with minimal human intervention. **Example:** Risk3Sixty, Resolver

Panel Discussion

Panel Discussion

JONATHAN COLOGNESI

Assurance Principal

jcolognesi@bdo.com

MARK MELNYCHENKO

Privacy Technology Practice Leader

mmelnychenko@bdo.com

MATT HANSON

Forensics Managing Director

mhanson@bdo.com

WAYNE ANDERSON

Cyber, Data Security and Privacy Director

wanderson@bdo.com

CONTACT US ▶

About BDO USA

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.