KROLL

Cyber Risk

Elite security leaders uniquely positioned to deliver end-to-end cyber risk solutions worldwide

Manage Cyber Risks Seamlessly with Kroll

How do you manage cyber security when virtually every area of your organization is digitally interconnected?

Today, beyond the risks associated with malicious insiders and outsiders, cyber security must also be viewed through the lens of “unintended consequences.” From system upgrades or a move to the cloud to applications meant to improve the customer experience to integral third-party relationships, one misstep can cascade into multiple threats, like wire fraud, ransomware, data breaches, and more.

Kroll’s elite cyber security experts can help you with every facet of cyber security. With years of public and private sector experience and law enforcement service, our experts provide invaluable guidance at any point in the cyber security continuum.

Kroll’s expertise managing thousands of cyber security engagements worldwide, backed by the diverse backgrounds of our experts, helped build the framework for a defensible cyber security strategy in five pillars. Strengthening these pillars helps your company develop an effective narrative in the event of an incident, including considerations such as:

- “We have performed a threat-based assessment focused on the type of data we store and transact.”
- “We’ve taken reasonable measures to protect our data from the threats that are most prevalent to our type of business.”
- “If an attacker does infiltrate our network, they would have to take extraordinary measures to bypass our security.”

Kroll’s cyber experts can help you build processes, training and contingencies, to develop, implement and enforce your strategy, and respond with speed and accuracy when needed.

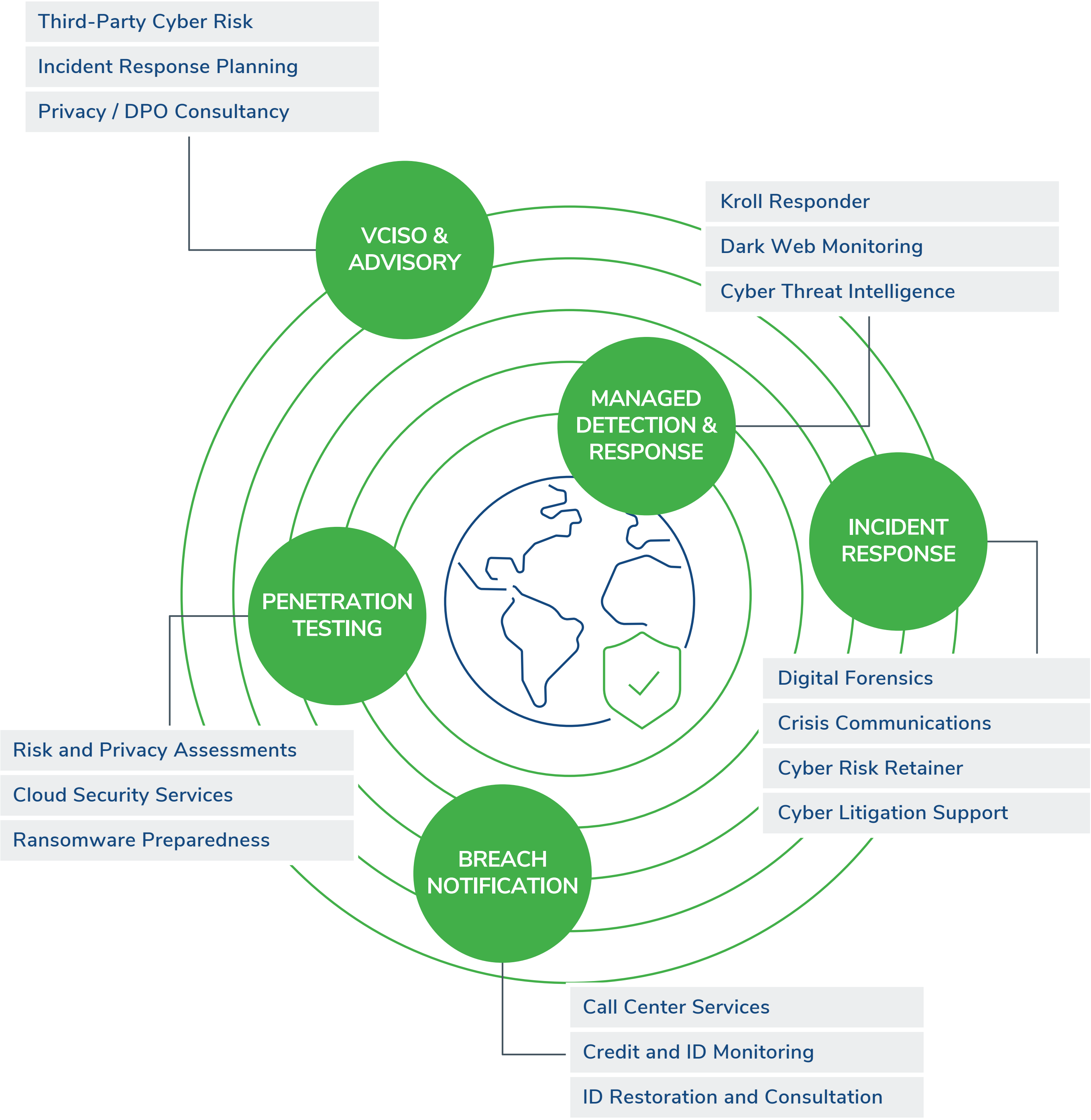
FIVE PILLARS OF A DEFENSIBLE CYBER SECURITY STRATEGY

An attacker with enough time, commitment and resources will eventually get into any network. The measure of a strong information security strategy, then, is the ability of a company to rapidly detect when an incident happens and effectively respond to it. Kroll’s unique ability to deliver end-to-end cyber risk solutions helps develop and strengthen a narrative for when (not if) an incident occurs and to prepare well in advance.

The five pillars consist of:

- Governance
- Policies and Procedures
- Infrastructure and Standards
- People and Training
- Relationships

PROTECT. DETECT. RESPOND



KROLL AT WORK – SELECT CASE STUDIES

IP Theft: Smart Car Startup

SCOPE	ISSUES	WHAT KROLL DID
• A smart car startup was being sued for theft of intellectual property (IP) by the executive team's previous employers. • Kroll investigators were engaged to forensically examine every device in the organization.	• Investigators needed to determine which machines and custodians (if any) had access to the IP in question. • Devices needed to be collected and analyzed with minimal business interruption.	• Forensically imaged 230 hard drives beginning on a Friday night and ending Sunday morning. • Extracted from all devices and processed 10 TB of data into a Relativity workspace that deduplicated down to approximately 2 TB. • Structured analytics operations, such as email threading, and conceptual analytics indexes were utilized to document clustering and concept searching.

Unauthorized Access: Regional Healthcare U.S. Provider

SCOPE	ISSUES	WHAT KROLL DID
• Provider noticed suspicious database queries made over four-six weeks and contacted Kroll per insurance company's guidance. • Cyber investigators were needed to validate whether queries were unauthorized, eject bad actors and eliminate any persistence.	• Incident response team was concerned about not alerting the actor to avoid punitive action, such as ransomware. • Needed to determine whether and how much PII/PHI was exposed by examining several mailboxes. • Outside counsel needed a detailed evaluation of the extent of the compromise to assess HIPAA and/or PIPEDA impact.	• We deployed EDR within two hours of engagement, to kickstart forensics. • Flagged corrupt activity and contained the incident. • Identified initial impacted population of over four million (mn) records and reduced it to 2.4 mn thanks to address validation procedures. • Notified everyone affected within three days, including state-specific letters in the U.S., Canada and bi-lingual call centers, delivering ID and credit monitoring. • Hardened configuration for Microsoft Office 365 and additional cloud services. • Client hired Kroll for ongoing virtual CISO services.

Cyber Incident Leadership: Southeast Asia Regional Bank

SCOPE	ISSUES	WHAT KROLL DID
• The information security team of a Southeast Asia Regional Bank noticed large-scale unauthorized access across several sensitive systems, which needed immediate response. • Due to the scope of the issue, the bank hired four regional firms to handle incident response, but little was accomplished.	• The bank's COO quickly recognized that the lack of leadership and experience was responsible for the poor performance. • They reached out to Kroll to amend the situation and manage the investigation.	• Provided oversight of the two remaining vendors on the engagement and led the investigation. • Guided internal team on evidence preservation and communicated with counsel. • Delivered post-incident guidance and local support to harden bank's systems • Provided SOC monitoring and training.

SWIFT Fraud: Middle Eastern Bank

SCOPE	ISSUES	WHAT KROLL DID
• Over $10 million identified as suspicious SWIFT transactions. • With several critical servers and workstations sabotaged despite EDR software deployed, the bank needed an incident response partner in the same time zone that could identify the root cause and remediate any potential compromise.	• Kroll needed to review thousands of SWIFT transaction logs and access details in a limited timeframe. • Malicious scripts had been buried deep within systems and could give attacker means to deploy ransomware.	• Took over monitoring of EDR software across ~3K endpoints to hunt malicious behavior. • Identified several command-and-control IPs and URLs, downloading malicious tools across many servers for over a year. • Removed automated rules on popped exchange servers that blocked emails containing "swift" and "case" keywords. • Provided full remediation and restoration of the bank's systems. • Client requested we continue to provide managed detection and response support, yearly penetration testing,red team exercises and physical security assessments.

MAKE CONFIDENT SECURITY DECISIONS

We know what is at stake and provide critical security insight to help organizations strengthen their privacy and information security programs. From incident response to risk assessments, and complex forensics to breach notification and litigation support, Kroll's cyber experts can help at every step on the way toward cyber resilience.

GLOBAL CYBER EXPERTISE

Many of our cyber professionals bring years of unique experience from their former service with large enterprises as well as law enforcement and regulatory agencies:

- Federal Bureau of Investigation (FBI)
- Interpol
- U.S. Department of Justice (DOJ)
- Securities & Exchange Commission (SEC)
- U.K. Intelligence and Policing
- U.S. Department of Homeland Security (DHS)
- U.S. Secret Service (USSS)
- U.S. Attorney's Office

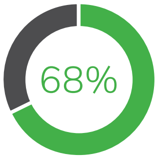
DID YOU KNOW...

Kroll works on ...

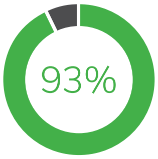
3200+

Cyber events per year for clients ranging from Fortune 100 to medium-sized businesses.

Kroll works with over...



of the Fortune 100



of the AM Law 100

Kroll has a dedicated insurance team for insurance and legal channels, with extensive relationships with 60+ cyber insurance carriers and exclusive benefits to insureds.

INDUSTRY RECOGNITION

CREST has accredited Kroll as a global Penetration Testing provider

Kroll is certified as a Global PCI Forensic Investigator (PFI) company

Kroll recognized as a Representative Vendor for Digital Forensics and Incident Response (DFIR) and Managed Detection and Response (MDR)

Kroll named a Global Leader in Incident Response Readiness

TALK TO A KROLL EXPERT TODAY

About Kroll

Kroll provides proprietary data, technology and insights to help our clients stay ahead of complex demands related to risk, governance and growth. Our solutions deliver a powerful competitive advantage, enabling faster, smarter and more sustainable decisions. With 5,000 experts around the world, we create value and impact for our clients and communities. To learn more, visit 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.