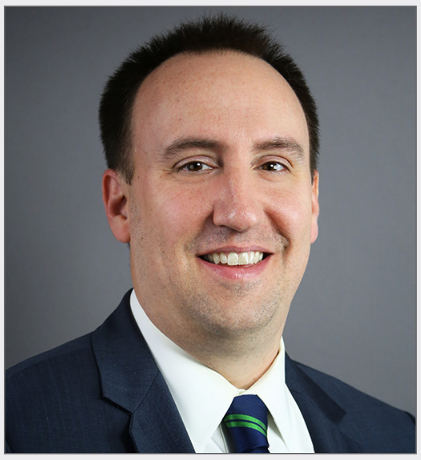
A Roundtable Discussion

CYBERSECURITY:

Protecting Data in An Era of Vulnerability

CHRIS CRONIN
Partner and ISO 27001 Auditor
HALOCK Security Labs
ccronin@halock.com
847-221-0202

DANIEL L. FARRIS
Partner
Fox Rothschild LLP
312-517-9269
dfarris@foxrothschild.com
312-517-9269



GREGORY J. LEIGHTON
Partner and Co-Leader -
Data Privacy and Information
Governance Practice
Neal Gerber Eisenberg
gleighton@nge.com
312-269-5372

JOEL MATHEN
Principal Consultant
Liberty Advisor Group
tritoncyber@libertyadvisorgroup.com
312-869-9707

October is National Cybersecurity Awareness Month, a collaborative effort that began in 2004 involving the National Cybersecurity Alliance and the U.S. Department of Homeland Security.

While total breaches were down in 2017, attackers are changing tactics. Where servers and workstations once took priority, threat actors are now directly targeting mobile applications and users to break networks and compromise data.

Four Chicago-area cybersecurity experts shared their thoughts with Crain's Custom Media on this ever-changing landscape, including what organizations can do to keep their workplaces, employees and customers safe.

CHRIS CRONIN is a partner at HALOCK Security Labs and chair of the DoCRA Council, a not-for-profit that authors, maintains and distributes standards and methods for analyzing and managing risk. He is an ISO 27001 auditor and author of CIS RAM, an information security risk assessment method. He uses his background in technical operations management, audit, legal research, and security management to find practical, defensible security solutions for clients. Away from work, he serves on multiple boards and advisory committees.

DANIEL L. FARRIS is a Chicago-based partner and co-chair of the technology practice at Fox Rothschild LLP, a law firm with more than 900 attorneys in 27 offices nationwide. A former software engineer and network administrator, he is fluent in privacy, data security, infrastructure and technology matters, also understanding how technology enables a company's operations and creates competitive advantage. In 2017, The National Law Journal named him to its list of Trailblazers in Cybersecurity.

GREGORY J. LEIGHTON is a co-leader of the data privacy and information governance practice at Neal Gerber Eisenberg, a Chicago-based law firm. A Certified Information Privacy Professional and a Certified Information Privacy Manager, he also is a registered patent attorney, working with clients to resolve controversies regarding intellectual property rights across a wide array of technological areas. He is a board member of the Illinois Legal Aid Online organization, which uses technology to increase access to justice.

JOEL MATHEN is a principal consultant at Liberty Advisor Group, a Chicago-based advisory and strategic consulting firm. He is a veteran in leading global projects for top-tier federal and Fortune 500 clients, emphasizing strategic planning, operational execution, risk assessment and intelligence analysis. He uses his technical, operational and industry expertise to help businesses achieve their strategic goals, and spent several years in Asia working on national security projects for the U.S. government.

What role does your firm play in improving cybersecurity?

Joel Mathen: We're a strategic consulting firm that partners with clients to solve complex business issues and improve enterprise value. We offer a suite of business threat intelligence products and services, as well as cyber monitoring solutions. Our team has a proven track record in business and technology transformation, data analytics, business threat intelligence, and mergers and acquisitions.

Chris Cronin: Information security consulting firms typically come in two flavors–those that diagnose and prescribe and those that implement. We do both. We're trusted security advisors to clients, helping them define their acceptable level of risk and establish "duty of care" for cybersecurity.

Daniel L. Farris: Law firms provide two key services–as advisors on a range of regulatory compliance and risk mitigation matters, and as recipients of highly sensitive client data. We strive to be leaders among our legal industry peers in the adoption and deployment of best-in-class security measures.

Gregory J. Leighton: We help clients develop programs to maximize the value of their data, while minimizing associated risks and costs. It begins by understanding their business needs and vision. We also help clients negotiate better insurance coverage and help guide them through the insurance claims process, if needed.

How can a company decide whether it's "secure enough" based on its industry, environment and other factors?

CC: Regulations, security standards, and judges all use "**reasonable risk**" as their determination of what's "secure enough." This frustrates people because authorities have not been specific about what "reasonable risk" means until very recently. CIS,® the Center for Internet Security, has just published its risk assessment method, called **CIS RAM**, that shows exactly how to determine whether you're "secure enough," and in a way that lawyers, regulators, business executives and information security practitioners can all agree.

DF: Information security, privacy compliance and risk mitigation are ever-evolving and incremental. The question is one of risk, weighing factors such as the amount, nature, sensitivity and use of personal data; the industry in which a

ASSESSING SECURITY

> *"A decision that a company is 'secure enough' is an inherently flawed assessment. A company's threat surface, threat actor's focus and techniques are constantly in flux. The question should be, 'Are we more secure than yesterday?' and 'What measures are in flight to become more secure tomorrow?'"*
>
> **JOEL MATHEN,** LIBERTY ADVISOR GROUP

company operates; geographic scope; regulatory enforcement and oversight; disclosure and consent; and the value of the data at issue. While perfection is the enemy of progress, making frequent, incremental changes and adapting to a continuously changing security landscape should be every company's focus.

JM: A decision that a company is "secure enough" is an inherently flawed assessment. A company's threat surface, threat actor's focus and techniques are constantly in flux. The question should be, "Are we more secure than yesterday?" and "What measures are in flight to become more secure tomorrow?"

In light of recent cyberattacks, have you changed the strategies or advice you offer companies dealing with the new reality?

DF: Our strategies evolve with each emerging threat. For example, the recent rise of ransomware—which encrypts and locks your data until you pay the ransom—has changed how we advise clients on cybersecurity, and how we ourselves handle network/data segregation and redundancy. Improving employee training to spot, but not respond to, suspicious emails is a good strategy for dealing with the influx of ransomware and phishing attacks. Another is to have strengthened data governance principles, like strong backup policies, so that minimal data is lost and users aren't crippled by lost access to systems due to a ransomware attack. Helping companies shift from reactive to proactive practices and securities has gone a long way with helping our clients be better prepared for cyber-attacks.

JM: Our strategy remains focused on mitigation efforts most aligned with detection and prevention rather than post-attack response. When looking at highly reported incidents such as ransomware, despite the frequency of attacks, there are some fundamental and consistent steps that firms can take to minimize their attack that don't require a huge alteration in strategy. This can include high-impact, preventative initiatives such as ensuring critical systems are running supported versions that have been patched, reducing privileged account holders, and ensuring that back-ups of critical files and systems are being made. Theoretically, an extortionist's effectiveness is immediately rendered moot if the victim was proactive and had already prepared a back-up to any data that was seized.

CC: Our mantra has been, "Log everything you can, starting with what will most likely go wrong." It's what our disappointed forensics experts say when a breached client explains that they have no logs to show us. But another reason why logs are always relevant is that we always find new techniques to detect and report suspicious behavior. In the past five years the information security community has found new ways to detect advanced malware, dangerous servers, suspicious people and unusual user behavior. Of course, this means that you need to analyze your risks so that you understand what's most likely to go wrong. But this is one of the reasons why risk assessments are so commonly called out in regulations.

What are some key elements and issues to be addressed in a cyber incident response plan?

CC: The National Institute of Standards and Technology's Cyber Security Framework tells us to identify our information assets, protect them using controls, detect suspicious behavior, respond according to a plan, and recover after the incident. As you design your plan, ask what you know about your environment—what systems and applications are there? What do you allow there? How would you discover things that aren't normally there? Then ask what kinds of logs you'll need to investigate the incident. A well-written and well-rehearsed plan is fundamental, but also prepare for the knowledge and resources you'll need on hand so your response is successful.

DF: Roles and responsibilities, escalation procedures, key outside vendors, periodic audit and testing obligations, reporting triggers and recipients, and relevant regulators are just a few things that should be addressed. Testing and exercising are particularly meaningful. Just as you don't want to be looking for the nearest exit when the fire alarm sounds, you don't want to be reading your incident response plan for the first time once a breach is detected. Table-top exercises are a great way to ensure that every person and department with delegated responsibilities under the plan is able to quickly execute and perform his or her duties when necessary.

GL: The most effective plan starts with an established and well-trained team that has practiced how it will handle a data incident to

minimize its potential impact on an organization's operations and reputation. In the event of a security incident, businesses need to have a trusted advisor to guide them through all phases of investigation, remediation and notification under applicable laws and regulations. The plan should detail both short-term actions and long-term actions, delineating everything that needs to happen to execute a prompt and comprehensive response. At the same time, it should define strategy regarding filing cyber insurance claims, reassessing vendor contracts, and avoiding or resolving enforcement actions to achieve the most favorable results. The most prepared organizations also will have planned for the breach by having established breach coaching and other training for all users, including breach simulations and penetration testing. They'll have relationships with vendors who can advise them on legal obligations that may arise from the incident, as well as with the forensic teams who will determine how the breach occurred.

JM: A plan must be detailed, but flexible, and should include mechanisms to consider unplanned roles and responses. Clear and practiced communication is critical during incident response—which more than any other cybersecurity or IT function, involves the entire company. Cross-functional preparation, testing, exercise and execution in an actual event is critical; its value cannot be overstated. And while not strictly part of a plan, continuous testing is important. Organizations are people, and people are going to execute a plan only as well as they've been trained.

What's your advice about purchasing cybersecurity insurance?

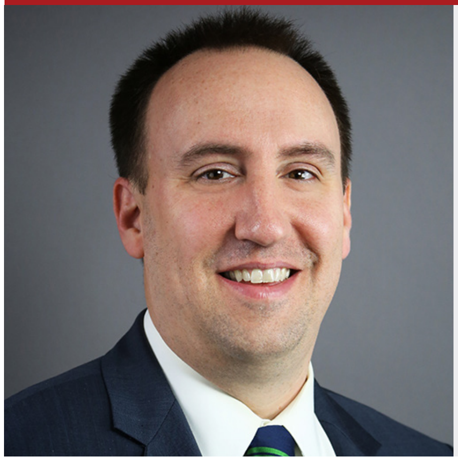
DF: Get it, but know what you're getting. Fit is critical for cyber liability insurance. Make sure your organization has the right coverages and levels given the amount, type and uses of your data. Many cyber liability policies exclude the exact risks you may be hoping to cover. For example, depending on the carrier, your company may need fraud, crime or even kidnapping coverages to address insider threats, phishing and ransomware. Review the exclusions carefully and understand how they may impact your specific risks. Get a coverage opinion from counsel if necessary.

GL: The effects of a business disruption related to a cyber-attack can significantly impact a company's bottom line. Liability costs as well as system and data recovery can result in lost income and high costs of data recovery and remediation. Having insurance coverage available to pay for costs associated with liability issues and to be available during any possible business interruption may prove essential to keeping an institution's doors open. Ranges of insurance coverage limits and amounts of deductibles vary widely, and so insurance coverage strategy should be included as part of an overall response plan.

JM: Many brokers, and therefore their clients, are pushing coverage options with little to no ties to the real cyber threats facing them. So, when a breach occurs, coverage fails to adequately respond to the event, leaving the buyer financially exposed. Our most important advice is not to assume that a long-standing broker relationship that's served you well in traditional lines of insurance is also providing you analytically sound and solid coverage options in cyber. Cyber insurance requires real expertise and nuanced coverage options to provide true coverage so that there are no surprises when the insurance is needed after a breach.

CC: Brokers and carriers are still trying to figure out how to estimate the probability and impact of cybersecurity risk to make the right insurance products for their customers. So, it's best to work with a broker who wants to work this out with you. Companies should find a carrier interested in "risk engineering." If you can measure your risk over time as you apply more controls, you can demonstrate to carriers that your risks—and therefore your premiums—should go down.

IMPACT ON M&A



> *"Once a complete picture of data security and privacy has been developed, companies can more accurately manage merger integration costs and understand long-term risks identified in a thoroughly executed due diligence review."*
>
> **GREGORY J. LEIGHTON,** NEAL GERBER EISENBERG

How are cybersecurity concerns impacting due diligence in M&A transactions?

GL: The increasingly connected world in which we live has made cybersecurity and data privacy a foremost concern when it comes to transactional due diligence. A good start to addressing cyber risk in a transaction begins with an assessment of cybersecurity and privacy compliance, including an audit of a target company's technologies, data and the policies and procedures that govern them. It's crucial that this be followed by review of third-party agreements that involve data-sharing and other digital access. It's also important to understand any past exposure to

LEGISLATION COMPLIANCE

"What's critical to understand about privacy regulations is that privacy is not security. Security is required to comply with these laws. The regulations go further, governing what is collected, from whom, how it is stored and used and with whom it can be shared."

DANIEL L. FARRIS, FOX ROTHSCHILD LLP

data breaches to ensure that vulnerabilities have been addressed. Once a complete picture of data security and privacy has been developed, companies can more accurately manage merger integration costs and understand long-term risks identified in a thoroughly executed due diligence review. We also help clients evaluate whether tails for cyber policies should be purchased as part of the transaction.

CC: The more pressing problem recently is, "How do I find hidden liabilities given our limited budget and time for due diligence?" Some acquiring companies try to resolve the uncertainty by adding a cyber insurance policy to the valuation calculation. While there's wisdom there, the acquiring company can also use some risk analysis more directly by asking whether the target company uses duty of care principles while managing their security program. Because regulators and judges set the price on liability, and because they evaluate reasonableness based on due care principles, a target company will likely hold lower liability by running their security program the way regulators and judges evaluate due care.

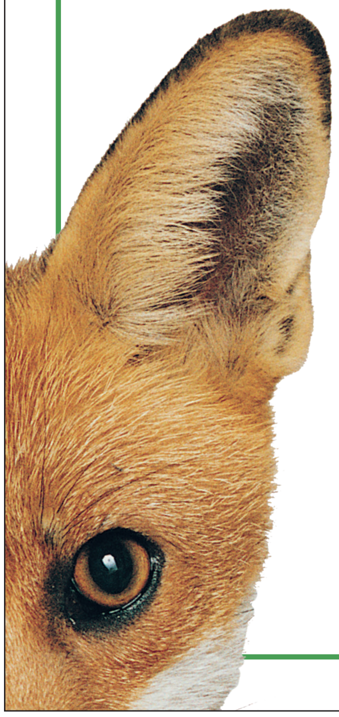
JM: Companies are most vulnerable when an M&A announcement is made public or when media speculation occurs around a potential deal. Attackers view a merger as an opportunity to exploit the weaker of the two entities, have their malware ingested into the new combined entity, and then gain access to a target with double the data to steal. Therefore, it's imperative to evaluate a target's information security posture during due diligence after the target selection phase. An assessment of a target's cybersecurity preparedness can equip a private equity firm or parent company with a better idea of what level of risk they may be inheriting. Including cyber in a due diligence helps identify any gaps going into the pre-merger planning phase and helps with negotiations down the line. Ultimately, it allows companies, both parent and target, to remediate gaps prior to public announcements so sensitive data can be appropriately protected. The major downside risk is that a company with sizeable investments in security could be compromised through the M&A process because vulnerabilities and exploits can be inherited and then are owned by the new entity.

DF: Privacy compliance has become a significant diligence issue in M&A transactions. Cyber concerns often impact negotiation of the transaction itself, whether that be through the inclusion of additional representations and warranties, holdbacks or other tails related to data security, indemnification requirements, and/or insurance obligations. Europe's new data protection law, the General Data Protection Regulation, or GDPR, has forced companies to be accountable to consumers for the use of their personal data. Acquiring companies are reluctant to take risks when corporate transactions may involve the transfer of sensitive personal data. M&A attorneys are more cognizant of these new requirements and are seeking guarantees that the target company will not put an acquiring company at risk due to lackluster data protection practices.

What should companies be doing to comply with current—and potential future—cyber-focused legislation?

JM: GDPR, SEC Guidance on Cybersecurity Disclosures, New York Department of Financial Services cybersecurity regulation are just a few of the regulations that can levy penalties and fines if companies are noncompliant. Organizations must review each regulation and thoroughly document their compliance. Globally, a few countries are discussing similar legislation to mimic Europe's GDPR to address their own citizen privacy rights. Companies with global customer bases would be well-advised to dedicate internal resources or hire external subject matter experts to stay abreast of these rules and regulations. Several U.S. states are also advocating for local cyber legislation, and we expect this space to continue to dynamically evolve at a fast pace.

DF: GDPR has been something of a sea change for companies operating in Europe and the California Consumer Privacy Act looks as though it will have similar effect in the United States. What's critical to understand about privacy regulations is that privacy is not security. Security is required to comply with these laws. The regulations go further, governing what is collected, from whom, how it is stored and used and with whom it can be shared. While the laws vary, there are some common denominators that can be used to harmonize compliance efforts. Data mapping exercises, for example, can help a company identify the information it has, where it is stored and how it is shared—all of which are key questions for compliance with laws like GDPR. Implementing privacy by design concepts and creating more



transparency and control for customers will only improve your organization's compliance posture.

GL: It's best to stay ahead of the curve by enlisting a trusted advisor or two to help ensure conformity, while the executives and board focus on other pressing needs. Good advisors, among other things, can help organizations stay on top of current and pending legislation. They can also work collaboratively to empower the cybersecurity program with qualified, vigilant leaders and the tools and processes necessary to excel. That way, should an event occur, prepared first responders will be able to take the right steps without delay. Because a cybersecurity program is only as strong as its weakest link, companies should select vendors that comply with their own rigorous standards. Finally, companies should remain vigilant by revisiting operations periodically and auditing their programs frequently.

CC: The open secret in regulations is that they're very business friendly, and they all demand the same thing–get to reasonable risk. Since Executive Order 12866 was signed in 1993, all regulations require a cost-benefit analysis to make sure that the public is protected from harm, but not by using safeguards that are overly burdensome. This shocks people to hear. But that's why the words "risk analysis," "risk assessment," "reasonable" and "appropriate" pop up so consistently in regulations. Risk analysis is how you do cost-benefit analysis, so do risk assessments the way regulators and litigators understand. Center for Internet Security has just published CIS RAM to show you how, and any new requirement that comes up in a regulation will be less intimidating.

What key cybersecurity elements should C-suite executives and board members be requesting from their IT departments and associated vendors?

GL: Executives and boards should meet on a regular basis with the lead person in charge of the organization's data breach response. Discussions should include deliverables such as a business risk assessment–rather than a risk assessment focused on IT systems–a risk mitigation plan, and the data breach response plan. All of these should ideally be updated and reassessed at least annually. The same executives and board members should request a budget assessment that allocates sufficient resources to alleviating cyber risk, including more than adequate resources to effectively staff the data management effort and enlist third parties for outside evaluation and assessment. Boards and executives can pursue excellence in cyber readiness by performing a benchmarking assessment to determine how the organization fares when compared with other market or industry leaders. Other potentially worthwhile elements boards should look for include cyber liability insurance, the establishment of frequent testing and reassessment protocols, and finding a vendor to help the organization track and comply with frequently changing regulations.

JM: The ROI of previous security decisions and investments is a calculable and statistically derived metric that executives and boards alike can point to in order to understand their real threat environment and the efficacy of past and future security decisions. Not having had a breach is no longer an adequate benchmark of good security. As more leaders correctly espouse the "if, not when" mentality to cybersecurity, reporting number of attacks-blocked statistics is approaching irrelevance because the benchmark loses all value the moment a breach is successful.

C-SUITE INVOLVEMENT

"Executives own cybersecurity, and therefore must communicate to any team that can create a risk to information and systems—which is everybody—what the organization's responsibilities are for protecting others and for protecting the organization's mission and objectives."

CHRIS CRONIN, HALOCK SECURITY LABS

CC: Executives own cybersecurity, and therefore must communicate to any team that can create a risk to information and systems–which is everybody–what the organization's responsibilities are for protecting others and for protecting the organization's mission and objectives. They must articulate what level of harm they'll tolerate and what they won't tolerate. Then they need to work with experts to determine how to measure their performance against those criteria. Finally, management teams need to provide metrics and aggregations or key risk indicators that demonstrate how well the controls work, and how well they're trending toward acceptable risk. If this sounds lofty, then ask how businesses have managed to do this already with financial reporting, quality management, team performance and more.

DF: This is better framed from the perspective of "What should IT and information security be requesting from C-suite executives and board members?" The answer is full support and acknowledgement of the company's cybersecurity efforts. Data protection will never be a pillar on which a company stands if executive leadership doesn't encourage its development and stand behind the teams that implement the company's data protection policies and procedures.

HALOCK®

Solutions We Offer

SECURITY MANAGEMENT – Prioritize and optimize security investments—applying just the right amount of security to protect your organization's mission as well as satisfy compliance requirements and corporate goals.

- **CIS RAM –** CIS (The Center for Internet Security) and HALOCK Security Labs have co-developed the CIS Risk Assessment Method (RAM) to help organizations justify investments for reasonable implementation of the CIS Controls. CIS RAM helps organizations define their acceptable level of risk and to prioritize and implement the CIS Controls to manage their risk.
- **RISK ASSESSMENTS –** Assessment of risk regarding your critical assets and the impact of threats and vulnerabilities on your corporate goals.
- **REQUIREMENTS & GAP ASSESSMENTS –** Harmonizing applicable security laws, regulations, and contractual requirements and conduct a GAP Assessment to clearly identify your current compliance and security state.

COMPLIANCE SERVICES for PCI DSS, HIPAA Security Rule and Meaningful Use, Massachusetts 201 CMR 17.00 and NYDFS Part 500 state breach laws, Gramm Leach Bliley, NERC CIP, ISO 27001, FISMA, GDPR and more.

- **HIPAA** – Helping to ensure that IT security investments are "reasonable and appropriate" as HIPAA and Meaningful Use require.
- **PCI DSS** – Guiding organizations through the process of PCI compliance and what is best for your organization.

PENETRATION TESTING – Checking the effectiveness of your existing security controls externally (remote) and internally (onsite).

- **EXTERNAL NETWORK** Assess the security of perimeter defenses of the hosts and services exposed to the internet.
- **INTERNAL NETWORK** Assess the security of internal private networks and hosts to assess what a malicious individual could compromise from within your environment.
- **INTERNAL WIRELESS** Assess the adequacy of wireless security controls designed to protect unauthorized access to corporate wireless services.
- **WEB APPLICATION** Comprehensively evaluate critical web applications using multiple levels of access for web application security vulnerabilities.
- **REMOTE SOCIAL ENGINEERING** Validate the effectiveness of user security awareness and incident response processes, primarily through phishing attacks.
- **ONSITE SOCIAL ENGINEERING** Assess the effectiveness of physical security controls, employee response to suspicious behavior, and validate that network security controls cannot be bypassed by establishing an onsite presence.
- **REMEDIATION VERIFICATION** Plan to identify, restore and rebuild, and verify affected network infrastructure, applications, and systems.

INCIDENT RESPONSE AND FORENSIC SERVICES – Provides guaranteed response times and digital forensic services via a 24/7 hotline and retainers for asset and cloud based investigations.

- **INFORMATION SECURITY MANAGEMENT –** Implementing a security management framework, based on ISO 27001 principles, that has the right size and scope for your needs.
- **ISO 27001 CERTIFICATION –** Assisting your organization in achieving ISO 27001, the globally recognized certification using our proven approach and expertise.
- **POLICIES & PROCEDURES –** HALOCK's proprietary policy development methodology and Security Policy Library can help you create, measure, and maintain the documentation you need.
- **SECURITY AWARENESS TRAINING**
- **CISO ADVISORY SERVICES –** You may not need a full-time Chief Information Security Officer (CISO) or you may not have the appropriate resources to fulfill that function. Let HALOCK be your Virtual CISO and leverage our expertise for your security management needs.

INCIDENT RESPONSE READINESS PROGRAM – Assessments, formalized planning, and training to respond to incidents using a structured process.

- **INCIDENT RESPONSE PLAN DEVELOPMENT –** Well-documented approach in handling threats to critical infrastructure and data within an organization.
- **INCIDENT MANAGER TRAINING –** Teaching the incident response team on the documented incident response plan with instructor-lead, scenario-based tabletop exercises.
- **INCIDENT RESPONSE TECHNOLOGY REVIEW –** Assessment of in-place security solutions that could assist with an incident management process — monitor, detect, log, correlate, etc.
- **FIRST RESPONDER TRAINING –** Training on how to preserve evidence for investigations using a provided set of tools.
- **COMPROMISE ASSESSMENT –** Hunting and reporting on active threats, unwanted applications, and behaviors within an organization.

WORKFORCE – HALOCK's expertise, network and insight to help you find the perfect infosec professional for your organization.

SECURITY ENGINEERING PROFESSIONAL SERVICES – Assistance with designing and deployment of on-premise and cloud security solutions.

- **SECURITY ARCHITECTURE REVIEW –** In-depth "as-is" or a "to-be" security assessment of the design, configurations, and controls of an organization's infrastructure.
- **SECURITY THREAT MONITORING –** Expert analysis, alerting, and guidance for security threats identified with HALOCK provided security tools.
- **SOLUTION EVALUATIONS FOR REMEDIATION –** HALOCK's security engineering team can hep develop a remediation plan and evaluate appropriate solutions ("safeguards") to treat unacceptable risks.
- **TECHNOLOGY/RESELL PARTNERS –** Resources for information, demos, evaluations, and discounts on a wide array of HALOCK handpicked security solutions.

HALOCK Security Labs
1834 Walden Office Square, Suite 200 Schaumburg, IL 60173
847-221-0200 | Incident Response Hotline: 800-925-0559
www.halock.com