K2 Intelligence

Investigations · Compliance Solutions · Cyber Defense

Financial Institutions and Asset Managers in the Cybercrime Crosshairs:

Developing Response Strategies to Complex Threats and Navigating Enforcement

K2 Intelligence CLE Materials

November 5, 2015

k2intelligence.com

New York · London · Madrid · Tel Aviv · Geneva

K2 Intelligence

Investigations · Compliance Solutions · Cyber Defense

K2 Intelligence is an investigative consultancy founded by Jeremy and Jules Kroll, the originator of the modern investigations industry.

Advising governments, companies and individuals, we help mitigate risk and maximize growth across the strategic, operational and reputational landscape.

K2 Intelligence conducts due diligence, investigative, analytic and advisory assignments all over the world. The firm employs a wide range of traditional investigative techniques—often amplified by the application of proprietary technology.

www.k2intelligence.com

The Convergence of Anti-Money Laundering and Cyber Security

Author: Thomas Bock of K2 Intelligence

This article was originally featured in the ABA Bank Compliance November/December 2015 issue.

Gone are the days when tracking a suspicious set of transactions was straightforward for the experienced anti-money laundering professional. Money was moved from one account and wired into another with clear origin and destination numbers, after which it might be moved again to other accounts or withdrawn.

What was once relatively simple is now becoming remarkably complex as banks continue to modernize with online services and alternative payment systems, including everything from prepaid cards, to mobile banking apps, to virtual currencies. This ongoing process of innovation is dramatically improving customer access and experience, but, at the same time, it is also opening new pathways for cyber criminals to infiltrate, steal, and cover their tracks on the money trail.

Earlier this year, a gang of hackers was found to have infiltrated more than 100 banks in over 30 countries. By using a “spear phishing” campaign, the hackers lured bank employees to unwittingly open deceptive emails, providing the hackers with access and the ability to insert malware that manipulated the banks’ software, accounting, and ATM systems. Over a two-year period, as much as $1 billion was siphoned directly from the banks, and the proceeds were layered into the hackers’ own accounts, in some cases using the SWIFT network.[1]

This is one of many examples taking place at the intersection of bank compliance and cyber security. It is a tangled web, as cyber criminals are using both traditional and alternative payment methods to aid illegal activities and mask identities while completing scams at light-speed. With this new breed of criminal, AML teams are facing their greatest challenges to date.

Regulators are keeping steady and aggressive watch over how well compliance teams are prepared to handle these new risks. Banks faced record fines and regulatory scrutiny of compliance programs in 2014, as U.S. and European banks paid nearly $65 billion in fines and penalties. [2] In addition, twenty of the world's biggest banks have paid more than $235 billion in fines and compensation in the last seven years for breaching a variety of financial regulations. [3]

Enforcement and investigations are increasingly challenging for regulators who are grappling with how to regulate a changing market with growing risks spread across cyberspace and the financial services industry.

K2 Intelligence is an investigative consultancy founded by Jeremy and Jules Kroll, the originator of the modern investigations industry.

Advising governments, companies and individuals, we help mitigate risk and maximize growth across the strategic, operational and reputational landscape.

K2 Intelligence conducts due diligence, investigative, analytic and advisory assignments all over the world. The firm employs a wide range of traditional investigative techniques—often amplified by the application of proprietary technology.

www.k2intelligence.com

designated compliance personnel and the same kind of AML procedures that apply to institutions handling fiat currency, but also detailed cybersecurity procedures. That is a reflection of how intertwined cyber crimes and the financial system have become. NYDFS is pioneering this regulation, but other regulations will follow.

Regulators are poised to take the same rigorous approach to investigating bank cybersecurity procedures as they have done with AML. At a recent conference, Former New York State NYDFS superintendent Benjamin Lawsky described cyber crime as a "huge threat to our financial system" and said "You are going to see a lot of action around cybersecurity and the regulation in that area." [5]

With these new regulations and risks, how can AML teams effectively leverage information about cyber criminals and identify suspicious transactions that are anonymous, fast, and hidden within a vast expanse of other data?

Unfortunately, there is no quick fix to managing these challenges. It requires a new mindset to understand the risks and then restructure and test programs to meet those risks. As a start, all banks, regardless of size, need to answer the following questions:

- How do your cyber and AML teams share information?
- Do you have a robust transaction monitoring system that is independently validated at least once per year?
- Are you prepared to review volumes of historical transaction data if regulators require you to do so?

Bridge the Cyber and AML Divide

The nexus of cyber crime and the financial system raises the question: with cyber-enabled crime making the movement of money harder to trace, shouldn't bank cybersecurity and AML teams work together? There is compelling evidence to suggest that these teams should be integrated, or even merged. Investigations of more traditional money laundering cases focus on account routing numbers. Cyber investigations focus on IP addresses and online traffic data. Merging internet data analysis with traditional AML techniques can be a powerful weapon to combat financial crimes.

As criminals move swiftly across cyberspace, bank AML teams remain grounded with traditional tools that are sure to miss key indicators. Banks need to strengthen resources to fight this battle through cooperation between cybersecurity and AML teams that currently operate in silos with minimal communication.

Before the prevalence of online banking, security cameras and other physical identification strategies helped detect suspicious behavior and locate criminals. Today, the IP address is key to identifying anomalies. If multiple transactions are made in different accounts from the same IP address, this is a clear indicator of suspicious activity. Why would multiple people in one house use the same computer to open accounts and conduct transactions? Clearly, more information is needed.

Sharing IP information is one example of how the AML and cyber teams can better coordinate. For thorough monitoring and risk management, suspicious customer activity

K2 Intelligence is an investigative consultancy founded by Jeremy and Jules Kroll, the originator of the modern investigations industry.

Advising governments, companies and individuals, we help mitigate risk and maximize growth across the strategic, operational and reputational landscape.

K2 Intelligence conducts due diligence, investigative, analytic and advisory assignments all over the world. The firm employs a wide range of traditional investigative techniques—often amplified by the application of proprietary technology.

www.k2intelligence.com

must be assumed to involve a data breach, while every data breach must be assumed to be a financial crime in the making.

Cyber crime frequently goes hand-in-hand with suspicious financial transactions. Bank accounts, credit card accounts, and ATMs are illegally accessed via “spear-phishing” emails or other “social engineering” ploys. Spear-phishing is when you receive an email that appears to be from an individual or business that you know, however, it is from criminal hackers who want your credit card and bank account numbers, passwords, and the financial information on your PC. Often, it takes an anti-money laundering mindset to detect the crime, or even to understand that a crime has been committed.

Transaction monitoring is a great place to start this integration. A typical assault on a bank starts with online customer data being stolen. But that data—account numbers, PIN numbers, social security numbers, debit and credit card numbers—has no value to the thieves until they can convert it into cash. This is classic money-laundering—now playing out online.

The AML team, having set up the rules and triggers that detect fraudulent transactions, can provide the cyber team with vital information about dates, times, dollar amounts, and the frequency of all sorts of anomalous activity. The two groups can then work together to cross-reference this information with any spikes in wire transfers, online purchases, ATM withdrawals, or other vulnerable banking activities. In this way, information flowing from AML to cyber can help detect and prevent attempts to monetize stolen data.

But the information needs to go in the other direction as well. Whenever the cyber team detects a breach in the bank’s firewall, the AML team needs to hear the alarm. The sooner they know about the intrusion, the sooner they can raise alert levels and heighten scrutiny of suspicious transactions.

Both teams can then walk back the incident to identify any early indicators. What happened in the preceding days, weeks, or even months? Was money moved into or out of suspect accounts? Are there patterns to the suspicious behaviors? While AML works the transaction information, Cyber can track the IP addresses involved in the incident. Working together, the two groups can accomplish what neither could by itself.

Cybersecurity and AML need to work together. The silos must be torn down. Each group can add significantly to the effectiveness of the other, and there is simply too much at stake for them to continue working in isolation. What is needed is a freer, more streamlined sharing of information between AML and Cyber.

We anticipate that regulators will also be calling for more sharing and coordination. In the future, compliance officers might see a cyber version of the Suspicious Activity Report, with which all financial institutions are familiar. It would be up to regulators to determine specific triggers for a cyber-SAR, but the format that banks use today could be adapted to collect information such as attack indicators, targeted domains, and tools, techniques and procedures used by the suspicious transactors.

K2 Intelligence is an investigative consultancy founded by Jeremy and Jules Kroll, the originator of the modern investigations industry.

Advising governments, companies and individuals, we help mitigate risk and maximize growth across the strategic, operational and reputational landscape.

K2 Intelligence conducts due diligence, investigative, analytic and advisory assignments all over the world. The firm employs a wide range of traditional investigative techniques—often amplified by the application of proprietary technology.

www.k2intelligence.com

Strengthen AML Processes and Procedures

At a time when AML and cyber are converging, and regulators are stepping up their enforcement activity, financial institutions need to redouble their efforts to strengthen and improve the core elements of AML programs. “Fix it and forget it” simply doesn’t work. Compliance officers operate in a dynamic environment, and annual assessments are critical to ensure that AML and cybersecurity programs are keeping pace.

Each year, every bank should be doing an overall risk assessment of the different lines of business, their varied customer profiles, and possible exposures. Programs quickly become outdated if a bank is not keeping up to speed with new money laundering schemes and ways that criminals interact with financial institutions. AML teams also need to improve understanding of the newest emerging payment systems to understand transaction patterns. Parameters must be reviewed and tested based on new risks to develop an effective set of rules to alert for suspicious activity.

As banks recognize the intersection of AML and cybersecurity, they will have a better ability to manage risks posed by new products, such as virtual currencies. Both teams must be involved in initial stages of the product development process. With a seat at the table, AML and cybersecurity officers can work together to help identify and implement proper controls. For institutions considering virtual currencies, it’s hard to envision banks not tapping the expertise of the AML and cybersecurity teams.

Checking the box is not enough. Programs need to be independently validated at least once per year. Enterprise-wide risk assessments should be conducted. Policies, procedures and KYC programs should be reviewed and tested, with extensive training for employees.

As banks move further away from in-person transactions, the criminals are quick to take advantage of more anonymity. It is imperative to modernize know your customer programs. The KYC programs of yesterday involved a checklist for bank branch employees to review with a customer that walked in the door, looking to open an account. Banks need to get to know and maintain contact with virtual customers. This requires training employees and evaluating progress on a consistent basis.

Get Smart on Data Analytics

Equally important to knowing your customer is knowing your big data. AML teams can’t make good decisions without a clear picture of the activity they’re monitoring and the risks associated with the data.

Banks hold on to massive amounts of data about customers. Customer information is critical to AML and KYC efforts, but holding too much outdated information poses a cyber risk. For example, many banks are holding on to information from former customers. This excess information poses an unnecessary cyber risk should that information be compromised. Banks are challenged to meet KYC requirements, but also have a firm understanding of what information is at risk for a cyber attack. It is critical for both AML and cyber teams to know the data and assess the risks involved.

K2 Intelligence is an investigative consultancy founded by Jeremy and Jules Kroll, the originator of the modern investigations industry.

Advising governments, companies and individuals, we help mitigate risk and maximize growth across the strategic, operational and reputational landscape.

K2 Intelligence conducts due diligence, investigative, analytic and advisory assignments all over the world. The firm employs a wide range of traditional investigative techniques—often amplified by the application of proprietary technology.

www.k2intelligence.com

Having the right analytics empowers compliance and cybersecurity efforts and minimizes the business disruption of scrambling to respond to challenging regulatory requests for specific data. A regulatory enforcement action can turn a compliance department upside down with a request for specific information found in hundreds of thousands of transactions.

As a recent example, a bank was tasked with responding to regulatory enforcement action that required data analysis for approximately 75,000 merchants relating to a review of pre-paid debit card transaction activity for a period of 18 months. With powerful data analytics used by intelligence and law enforcement, the bank was able to identify potentially suspicious behavior by analyzing transaction patterns. This has resulted in substantive, large-scale investigative follow-up.

Detecting anomalies in a sea of data is a daunting task, but somewhat more daunting is preparing and normalizing data before it can be analyzed. After multiple mergers and acquisitions, banks typically find a patchwork of data formats. Different systems are merged and there is no uniformity of data points to monitor abnormalities. Now is the time to review the integrity of data, before a regulatory investigation occurs.

Once the data is normalized, that is when the analytics can launch into action to analyze activity including dates, transaction parties and financial instruments used. Having high integrity data and access to sophisticated analytics is critical to preventing and preparing for regulatory investigations.

Bank compliance officers should be prepared for these actions with regulator-approved methodologies to clean up problems in data, prepare it for sophisticated analysis and identify anomalous behavior. It is more than having the right tools. It is having a process for data ingestion, cleanup and developing a system where it will be possible to analyze and see the transactions and the trends over a given period of time.

Modernizing AML

AML is more complex at the intersection with cybersecurity. Compliance has entered an era of convergence, where silos have become risks, rather than just inefficiencies. Increasingly, financial institutions will see the advantages of a strategic, integrated approach to sharing information among their cyber and AML teams. Collaboration enhances their value to the institution, so it makes sense to bring them together in a coordinated way.

Compliance officers' roles have never been more challenging. They need to modernize and strengthen teams and programs to prepare for current and future uncertainties. The sophistication and diversity of criminal schemes will continue to grow.

Regulators have already acknowledged this intersection and will be increasingly focused on cybersecurity measures. Banks that share information, understand and prepare for risks, test systems and strengthen programs will be in the best position for success.

K2 Intelligence is an investigative consultancy founded by Jeremy and Jules Kroll, the originator of the modern investigations industry.

Advising governments, companies and individuals, we help mitigate risk and maximize growth across the strategic, operational and reputational landscape.

K2 Intelligence conducts due diligence, investigative, analytic and advisory assignments all over the world. The firm employs a wide range of traditional investigative techniques—often amplified by the application of proprietary technology.

www.k2intelligence.com

Endnotes

[1] http://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab

[2] http://www.wsj.com/articles/no-more-regulatory-nice-guy-for-banks-1419957394

[3] http://www.ibtimes.co.uk/20-global-banks-have-paid-235bn-fines-since-2008-financial-crisis-1502794

[4] http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf

[5] http://www.americanbanker.com/news/law-regulation/nys-lawsky-unveils-final-bitlicense-regulations-1074667-1.html

ABOUT THE AUTHOR

Thomas Bock is Executive Managing Director and Head of the Anti-Money Laundering (AML) and Regulatory Compliance Practice at K2 Intelligence. He can be reached at tbock@k2intelligence.com.

K2 INTELLIGENCE: ADDRESSING CYBER RISK AT THE EXECUTIVE LEVEL

Ensuring the continuation of operations and minimizing the risk of loss due to cyber incidents is a critical management issue and one of utmost importance to the boards of public and private companies alike. The hardening of company networks with multi-million dollar security is no match for the ever evolving cyber security threats and threat actors. **Austin Berglas, Head of Cyber Investigations and Incident Response for the Americas** at **K2 Intelligence**, a corporate investigations firm with offices in New York, London, Madrid and Tel Aviv, talked to DIRECTORS & BOARDS about the cyber landscape and the steps that boards of directors and their executive teams now face to defend, detect, respond to, and recover from a cyber-attack or incident.

Directors & Boards: **Boards are scrambling to react to cyber threats globally, but every day we hear of another corporate breach. In some ways, is it too late to react?**
Austin Berglas: It is never too late to react. However, to minimize the associated operational, financial and reputational repercussions, it is best to enhance proactive and reactive capabilities before an attack is detected. With the number of successful cyber-attacks on the rise, the relevant question for companies is no longer if or when they will be attacked, but how prepared are they for the attacks going on within their walls right now. The speed and effectiveness with which a company recovers from a cyber-attack is directly proportional to the level of its preparedness for such events, and preparedness starts with good management. Organizations must ensure that all employees are continuously trained on and made aware of the most common types of cyber security threats.

D&B: **What can a board do first and foremost to demonstrate its due diligence in preparing for the inevitable hack?**
AB: The board needs to have a thorough understanding of the procedures and practices already utilized within the company to defend, detect, respond to, and recover from an incident. And, on an ongoing basis, they need to challenge management teams to keep exploring strategies and ways to improve their preparedness and incident response plans. But they can't stop there. The board needs to understand what the impact of a cyber-network attack would be against the company. What are the crown jewels, where are they hidden, who would find value in them, and how well are they 'walled-off' from intruders. And they must be willing to make the necessary investments to protect those assets.

Austin P. Berglas heads the U.S. Cyber Investigations and Incident Response practice at K2 Intelligence. His deep investigative experience spans counter intelligence, national security, criminal cyber investigations and incident response. Before joining K2 Intelligence, Austin served as Assistant Special Agent in Charge of the FBI's Cyber Branch in the New York Office, where he oversaw all national security and criminal cyber investigations in the largest cyber branch in the FBI. He can be reached at aberglas@k2intelligence.com.

D&B: **Some directors have lamented that it's too expensive to "back fill" systems to counter future attacks? How do you respond to this?**
AB: The "set and forget" methodology of hardening networks with high end, multi-million dollar security is not a guarantee against future attacks. Resources spent on network hardening and defense can be defeated by just one click of a malicious E-Mail. Boards can and must take the lead in pre-incident preparedness and employee education. One tool boards should insist upon are moderated, table-top exercises that enable management teams to learn process and procedures based on realistic, actual scenarios.

D&B: **As a director, should I be concerned if my competitor has been breached?**
AB: Yes. Frequently threat actors will target organizations in the same industry sectors simultaneously, often with increased phishing activity. Beyond knowing preparedness plans, the board should ask about industry information sharing platforms that might lead to early identification of threats and vulnerabilities.

D&B: **When a critical breach is detected, how should directors react?**
AB: Calmly. A solid incident response plan will enumerate who is in charge, what the reporting structure is, and what actions each management level (C-suite/legal/tech) will take during the incident. How, when and by whom notification is made to the board, shareholders, and customers should be part of this plan. The plan will also detail when and how to engage public relations and who the designated media spokespersons should be.

D&B: **What happens after?**
AB: Due diligence and learning necessitates questioning. Did the team exceed their capabilities to identify and manage the incident? How fast were they able to move to identify and contain the intrusion? Is there confidence that the methods used to scope and contain the intrusion were effective? What additional resources, such as outside personnel and/or equipment, would potentially be needed in the future? Conducting an after action review of your incident response plan is key.

K2 Intelligence

Investigations · Compliance Solutions · Cyber Defense

K2 Intelligence is an investigative consultancy founded by Jeremy and Jules Kroll, the originator of the modern investigations industry.

Advising governments, companies and individuals, we help mitigate risk and maximize growth across the strategic, operational and reputational landscape.

K2 Intelligence conducts due diligence, investigative, analytic and advisory assignments all over the world. The firm employs a wide range of traditional investigative techniques—often amplified by the application of proprietary technology.

www.k2intelligence.com

Why Banks Need Both Intelligence and Technology to Stop Cyber Attacks

As the recent revelation of a $1bn fraud against 100 banks across the world demonstrates, cyber attacks on banks are increasingly sophisticated in execution and international in scope – the gang which carried out the latest heist is based in Eastern Europe and China, according to research by Russian security company Kaspersky.

A so-called “spear-phishing” attack was carried out on targeted staff at a number of financial institutions, who were sent emails which tricked them into opening software files which allowed the cyber criminals to access the banks’ internal networks and learn how transfers were done. The gang also controlled ATMs remotely, to dispense money to awaiting accomplices.

“These attacks don’t happen over four or five hours, they’re not the whim of a lone teenager in a college bedroom,” says Oisin Fouere, K2 Intelligence’s UK managing director for cyber security. “There’s a distinct attack lifecycle which we identify as part of our pro-active monitoring: this begins with a reconnaissance phase which is repeated once they have accessed a company’s networks, to further identify the key systems they wish to target. At that point, the attacker either alters the system so it is no longer secure or finds a way to steal the supposedly secure data.

“Banks often only identify the security compromise once the frauds are being reported by customers. This identification process occurs at the end of the attack lifecycle. Banks need the ability to monitor and infiltrate the very underground groups which are planning and executing these attacks. Often however, they are still too reliant on pure technology-driven safeguards; they need to invest in intelligence-driven cyber security to supplement their technical controls.”

The groups carrying out cyber crime attacks “operate exactly like legitimate businesses – there’s an economic market model defining the attack strategy, maintaining resource costs, and ensuring margins for any profit generated,” says Fouere of K2.

The limitations of technology alone in preventing cyber attacks on banks are clear, because there are numerous examples of financial institutions being compromised: another large cyber break-in affected banks in the UAE and Oman in 2013, when a criminal gang stole

K2 Intelligence is an investigative consultancy founded by Jeremy and Jules Kroll, the originator of the modern investigations industry.

Advising governments, companies and individuals, we help mitigate risk and maximize growth across the strategic, operational and reputational landscape.

K2 Intelligence conducts due diligence, investigative, analytic and advisory assignments all over the world. The firm employs a wide range of traditional investigative techniques—often amplified by the application of proprietary technology.

www.k2intelligence.com

$45mn after being able to hack in to a database of pre-paid debit cards and over-ride withdrawal limits. In one ten-hour period, the gang and their accomplices around the world were able to withdraw $40mn in 36,000 transactions at cash machines in 24 countries.

“Anti-virus intrusion systems are looking for signatures of known activity, of previous attack methods – so when people design an attack from scratch, they can slip entirely under the radar,” says Fouere. “By gathering intelligence to keep abreast of new malware developments and trends , you’re more likely to identify that an attack will take place, or is taking place, because these groups operate within closed forums: they’re using the deep web, talking in closed groups or encrypted chatrooms. They need to communicate with each other and with whoever is funding the attack. And most importantly they outsource specific responsibilities when they don’t hold this skill in-house. It’s at this point we can pick up the indicators.”

K2’s intelligence analysts have the ability to monitor such communication in order to protect customers, and to warn them ahead of an attack taking place that they need to strengthen controls in a particular system, or close it down altogether.

However intelligence is used very much in conjunction with technological security, not as an alternative:

“Sometimes we may not know who is being targeted, but we know somebody is working on a custom Trojan [a malicious computer program], and we can create signatures for customers to be able to identify it if reaches their systems,” says Fouere. “Maybe nothing happens for six months, but then suddenly it hits their system and they have the right controls and response procedures in place.

“The other advantage of this match-up is that it then tells us which customers are being targeted by that particular group – that’s the benefit of having intelligence support in place as well as technological support.”

Spear-phishing, or the sending of fake emails purporting to be from within the same company or another legitimate source, to trick staff or customers into handing over secure details such as passwords and account numbers is “the most popular form of attack at present”, says Fouere, because it does not even require hackers to get past security systems; they simply have to persuade someone to open the door and let them in.

“Even in really technically savvy companies, people get emails that look like they’re from the IT department telling them they need to change their password, and they go ahead and punch it in,” he says. “Organisations have a responsibility to educate their own employees as well as customers. We would stress that an email is like a phone call – you need to authenticate who you are ‘talking’ to before giving away any secure information.”

K2 Intelligence is an investigative consultancy founded by Jeremy and Jules Kroll, the originator of the modern investigations industry.

Advising governments, companies and individuals, we help mitigate risk and maximize growth across the strategic, operational and reputational landscape.

K2 Intelligence conducts due diligence, investigative, analytic and advisory assignments all over the world. The firm employs a wide range of traditional investigative techniques—often amplified by the application of proprietary technology.

www.k2intelligence.com

For all the technology and intelligence a bank can purchase to try stay one step ahead of highly professional cyber gangs, it may seem absurd that one of the biggest threats they face is an innocent member of staff effectively opening the front door and letting the criminals walk straight past its security systems. It is, however, something that can be avoided with decent training and adequate vigilance, says Fouere of K2.

“Staff need both training and regular reminders,” he says. “On-going measuring of the largest concentration of people in your business who are vulnerable to this, and keeping on top of their susceptibility, is vital.”

Cybersecurity and Supply Chains: A New Risk Management Paradigm

Businesses should understand where the weakest links are in their supply chains and where their sensitive business data resides outside of their network.

BY JEREMY M. KROLL

Today, companies large and small are facing complex security and privacy challenges. Managing cybersecurity risk has become a leadership-level priority. We read about a massive data breach almost every day and are beginning to succumb to "breach fatigue" where every new breach seems to have less impact than the previous one.

What we are seeing, in our increasingly interconnected and globalized business world, is that security vulnerabilities have multiplied and are more diffuse. Before the advent of the Internet and the digitization of core business functions, a criminal would need to physically break into a company's stores or offices to steal customer information or credit card numbers. They were constrained by what they could carry or the time they could spend inside a building before being discovered.

In the age of persistent cybercrime and compromised data, criminals can breach a business' defenses from anywhere in the world. They steal valuable data from a company not only directly through company networks, but also indirectly through the network of a supplier. They buy access to compromised company credentials or other attack-kits that are tailored for specific industries or even specific businesses. And after securing ever-higher network access and credentials, they can remain undetected inside a company's systems for months or even years, continuously siphoning off valuable data and penetrating deeper inside a business' network.

VIRTUAL SAFE HAVENS

The black markets for hacking tools, credit card numbers, competitive intelligence, intellectual property and how-to guides to breach companies are proliferating. They are also becoming more sophisticated. These virtual bazaars are housed inside the Dark Net, a series of hidden websites and forums that are only accessible with such special anonymization software as Tor.

Cybercriminals and "hacktivists" buy and sell valuable information, ready-made vulnerabilities and data about individual companies inside these markets. And with more effective attack tools being developed and sold, hackers are gaining attack capabilities and intelligence they did not have before these markets existed. They can also sell valuable data they have stolen to other hackers after an attack has occurred. The availability of hacking tools and the corresponding diminished need for technical sophistication to perpetrate advanced and highly targeted attacks is a worrisome trend that is poised to continue.

It is from these virtual safe havens that many hackers have been planning and launching their operations. They target the most vulnerable entry points they can find. This means hackers often do not attack businesses directly, where they tend to be more fortified. They start by attacking the connected suppliers such as an HVAC vendor, the payment processor, the point-of-sale system, the law firm, or third-party service providers. For those

(Continued on page 70)

(Continued from page 69)

of us who help businesses profile their cyber risks and gather intelligence about how hackers are targeting them, these developments represent an escalation that many business owners have not yet fully grasped.

BREACHES ON THE RISE

The statistics on breaches are staggering and are trending in the wrong direction. According to the Ponemon Institute, which conducts independent research on privacy, data protection and information security policy, 43 percent of surveyed executives admitted their company had a data breach involving loss or theft of 1,000 or more records in 2014. That is up from 33 percent in 2013. When a third party is involved, it increases the average cost of a data breach by $14.80 per individual record, which adds up quickly when breaches involve thousands or even millions of compromised records.

The breach of Heartland Systems, a Fortune 1000 payment processor, in 2008 compromised 130 million debit and credit cards issued by more than 650 financial institutions. It was the largest breach of its kind at the time. It also presaged the environment we live in today. It highlighted, in a new way, the risks and costs vulnerable suppliers can impose.

We have seen millions of dollars in data breach remediation costs inflicted on companies such as Target and Home Depot. Less well-reported are the post-breach costs inflicted on small- and medium-size businesses. SMBs may not have the wherewithal to weather the costs of mitigating a breach, the decrease in sales, providing required customer notifications, fighting back against lawsuits or repairing their damaged reputation. These costs can force businesses into bankruptcy or to close their doors altogether.

Unfortunately we have also seen a disturbing trend of "blame the victim" when it comes to data breaches, even if the company was compromised through vulnerabilities at a vendor. The media reflexively direct its ire toward the business victimized and blame it for the breach, instead of blaming the criminals.

CHANGING SCOPE OF VULNERABILITIES

Given these realities, companies need a greater understanding of the full scope of their vulnerabilities. Business owners and operators may have complete trust and confidence in their own management and IT team to protect their internal systems. But do they have that same confidence in their vendors' security teams? Do they have any visibility into the threats and attack vectors facing their supply chain? Do they believe that their law firms and accounting firms, which house huge amounts of sensitive company data, can protect that information from exfiltration?

Do they know which of their suppliers have access to their systems either directly or indirectly? Do vendors have robust data protection policies? Have partners implemented comprehensive incident response plans and policies for notifying customers and clients about a breach? Do partners have a full understanding of their risk profiles? Do suppliers have cyber defense requirements for their own subcontractors and suppliers? If a partner is being evaluated as an acquisition, will vulnerable or already-infected systems be imported after the transaction?

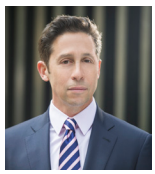
These are questions we have been asking our clients that they are often not asking themselves. Many companies still think about their IT security the same way they did when firewalls and antivirus software were all that was needed to secure company systems. Or they may be so focused about their own systems that they forget about how interconnected their businesses truly are. As many recent breaches demonstrate, the good old days of needing only to build the tallest walls and widest moats around networks are long gone.

OUTSIDE-IN UNDERSTANDING OF SUPPLY CHAIN RISK

Business owners should seek a richer understanding, from the outside-in, of the threats and malicious actors they face and the tactics those actors will employ. They also should know what kind of sensitive company information and compromised credentials are already exposed and are being bought and sold inside Dark Net marketplaces. Those efforts should complement the traditional pre-investment or vendor due diligence processes that businesses undertake when onboarding a new supply chain partner or evaluating a potential acquisition. These measures allow companies to plug vulnerabilities that might already exist.

Most importantly, businesses should understand where the weakest links are in their supply chains and where their sensitive business data resides outside of their network. That understanding comes from building a comprehensive risk profile and setting priorities around which risks deserve the most attention. Companies should also take extra precautions to ensure vendors and third-party service providers are doing everything possible to protect their partners, clients and customers.

As we see it, this is the new security and risk management paradigm that businesses face. And it is incumbent upon us all, across all industries, to foster cooperation and work even harder to ensure we can tackle these new threats together. ■



Jeremy M. Kroll is president, CEO and co-founder of K2 Intelligence, a cyber defense, compliance, due diligence, investigative and risk management solutions firm. Find him at jeremy@k2intelligence.com.