# FEATS OF STRENGTH



PROFILES IN SECURITY

Earning the right to be confident in IT Security


VOLUME 3 / ISSUE 1
APRIL 2015


K logix

LETTER FROM

# KEVIN WEST

CEO

## DEAR READERS,

In this issue's "Profiles in Confidence", we hear from Ravi Thatavarthy, the Head of Security at iRobot, and Phil Curran, the Chief Information Assurance and Privacy Officer at Cooper University Health Care.

Both of these professionals discuss their roads to success, leadership styles, and achievements that have enabled them to become confident security leaders.

Are you a business leader like Ravi and Phil? We explore that topic and more in this issue of Feats of Strength.

**Kevin West**

# Are you a **Business Leader?**

### Questions CISOs Need to Answer

As information security has moved to the forefront of general interest news, we have suddenly seen much more scrutiny of corporate security strategy and the goals of security leaders. For the first time, the Wall Street Journal which is among the most read business publications in the world, provides a weekly security news update. Many say this is the year of cyber security, but more likely, it is the year of the Chief Information Security Officer. The CISO, and his/her strategy, has never been so closely studied. With attention, comes great opportunity, and so this is the CISOs chance to up-level their role in business, and their impact in the board room. All of this depends on the CISO adopting and implementing the right approach for their business.

We have noticed that CISOs are coalescing around two different approaches to security programs.

The first group is focused on the noise.

They react to the threat landscape and take a defense-first approach, striving for 100 percent security. They focus on technology, policy, and procedure with a goal of absolute elimination of threats.

The second group of CISOs focuses on business performance.

They take a more strategic tact and are led by business similar to their peers in sales, marketing, and finance. They seek to enable business progress with security programs. They are more engaged with their business counterparts, not just when a breach occurs.

**How do you know if you are in this second group of business-focused security leaders? Ask yourself these questions:**

#### 1. Do you have regular, two-way communication with the board?

The board room is where important decisions are made and where strategy is set. Business-focused security leaders have a role in the board room as an expert, a resource, and a visionary. They define the company's security program as a forward-thinking program that limits risk while enabling optimal business performance. Business-minded CISOs come to the boardroom for regular conversation and influence business

practices and strategy, not to update on threats, hacks, and defensive schemes.

### 2. Do you know your organization's top five business objectives for the year?

Business-savvy security leaders can impact growth and productivity in a positive way by aligning their efforts with corporate strategy. For example, if a company's priority is customer acquisition, then the security team must align initiatives in a way that supports sales and marketing strategies for growth that does not impede workforce productivity. Business-focused security leaders are able to articulate sophisticated security processes as a competitive differentiator to potential new customers.

### 3. Do other business leaders in the organization proactively seek your counsel?

Communication and collaboration with other business leaders is a vital part of a successful security program. A business leader wields indirect influence to great effect, and is called upon by other organizations to provide counsel. If you are routinely brought in for consultation at the earliest stages of new programs, products, and corporate direction, then it is likely others are recognizing you as a business leader.

### 4. Is your team comprised of business-savvy technologists?

Any CISO will tell you that the strength of their program is directly linked to the strength of their team. While technology awareness and security product expertise matter, to be truly impactful, security teams must collectively understand business goals, be able to communicate effectively with business users, and position themselves as business enablers. These types of teams work from the same mission as the rest of the company and seek opportunities to strengthen programs with security elements.

Business-savvy security executives are focused on optimizing performance, not reacting to *just* the noise. This means they are continuously measuring their program against business goals. These security leaders are able to drown out the noise – those attacks and threats that dominate news headlines and have the potential to sway a security program off-track. At the end of the day, these leaders ask themselves one important question, "How can I security enable my business to achieve its revenue potential?"

"Have a business-centric vision. As CIOs look to create change within their organizations, strategic vision and execution will be essential. CIOs [at the WSJ CIO Network] highlighted the importance of speaking the language of business, tailoring the message to stakeholders and using terms they're comfortable with. Once CIOs have communicated and executed on their visions, it's crucial to measure success. After that, rinse and repeat."

*Reported by Steven Norton in the Wall Street Journal on February 4, 2015*

## THREE QUICK WAYS TO GAIN INDIRECT INFLUENCE

1. **Network** – Get out of the IT department and meet with business executives on their terms. Ask them about their priorities and challenges.
2. **Speak their language** – Leave technical jargon in the IT suite and focus on business value and risk, two areas all business leaders can understand.
3. **Be Flexible** – Ensure security programs do not impede worker productivity and be willing to make changes to security processes when needed.

# PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs

## RAVI THATAVARTHY

Head of Security
iRobot

"Being new to iRobot, the most important thing I need to do is establish indirect influence. I will do this by establishing key relationships with business executives, making an effort to get to know the people of iRobot, and understanding the culture. When they consult with me on a major project, or invite me to a project kick off, I know I have established indirect influence."

## FOUR FACTORS TO SUCCESSFUL SECURITY PRACTICE

Previously the Head of Security at Haemonetics, Ravi Thatavarthy now heads the security team at iRobot Corporation, a leader in robotic technology-based solutions. When we spoke, Ravi had been at the helm of security for iRobot for only nine months, and still in the ramp-up and implementation phase of enhancing the company's security program. However, with years of experience and strong beliefs in his approach, Ravi has his game plan in place. At iRobot and other organizations he has worked at, he will follow these four key principles:

### Communication with the Board

The board at iRobot understands the business value of security, and considers it a strategic imperative, which makes communicating with them fairly easy. Ravi strives to use the same context every time he speaks to the board, and to provide examples and comparisons from similar businesses. He says, "To be successful with the board, always present a plan and an answer."

### Be in the People Business

Ravi's team strives to ensure that security is timely and provides "user delight". "User delight" means to avoid being a road-block or a drag on employee morale. To be in the people business you must understand the business goals of each department, from R&D to marketing,

sales, and beyond. Security teams may get bogged down in defending the company against threats, and as a result start to wrongly view employees as the bad guys. You must assume good intent. The R&D team just wants to do their job to the best of their ability.

### Be Part of the Solution, Not Part of the Problem

"We are here to ensure security, not to stop business productivity," says Ravi. We need to present business leaders with the risks, but let them make the final decisions in terms of the risk they are comfortable with. "If you project risk in the right spirit, in your role as an indirect influencer, you have done your job successfully."

### No Organization has Unlimited Budget for Security

Optimize the use of your existing security budget and leverage other efforts on top of that. Some security priorities have insufficient business value, so be creative to find funding for those efforts. Whenever possible, prioritize security with respect to business value.

"Be speedy, be flexible and be direct!" Ravi's approach to security comes down to business enablement. By networking with business leaders at iRobot and fostering a reputation for being accommodating, efficient and yes, likeable, Ravi reports that he is brought into more projects, which ensures security's place in the process.

"Some companies have huge security budgets and still get breached. For mid-size companies, the approach to security has to be about security awareness. Our employees have to be security aware, or else our program will not succeed."

**- RAVI THATAVARTHY**

## A BUSINESS-FRIENDLY APPROACH

"I was delivering a speech about my business-enabling approach to security, and specifically talking about social networks and other sites that may open the company up to vulnerabilities. You cannot block access to these sites without losing the trust, ear, and collaboration of the employees. Some people certainly disagreed with me about this at the conference! In fact, there was a lot of opposition in the audience, and some walked out in the middle of my presentation. A few CISOs argued that you could never get a stronger security posture when allowing these sites on the network. I disagree. Security cannot be accomplished by only technical controls! If it is, emplodyees will simply work to circumvent the rules; and then you are less secure than ever. Use technology on the defensive, but do not use it on your own employees."

# PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs

## PHIL CURRAN

Chief Information Assurance and Privacy Officer
Cooper University Health Care

### Phil's Key to Success

"I surround myself with smart people. Our team is constantly looking at the way we are working and if we can do it better. We meet with business leaders all the time, and we are constantly assessing how we can provide more value to them and be more valuable to the business."

## "IT'S NOT IF, BUT WHEN"

Recently, Phil Curran the Chief Information Assurance and Privacy Officer at Cooper University Health Care, was making his usual rounds when he ran into the CFO of the hospital. The CFO said, "I remember Phil - it's not if, but when." The quick exchange was positive proof that other senior leaders at the hospital were hearing and abiding by Phil's message of constant vigilance and preparedness when it comes to privacy and information assurance. "They (the board) are embracing information assurance as a strategic imperative," says Phil.

As a member of the hospital's audit committee, Phil has the ear of the Board of Directors on a quarterly basis. While major hacks and threats in the news may pique interest or spur specific questions from the board, Phil keeps them focused on ongoing information security awareness and preparedness by reminding them that "it's not if, but when." Outside of the Boardroom, Phil believes that face-to-face interaction and old-fashioned networking are vital to keeping security at the top of mind amongst business leaders who are managing budgets and making important decisions that may have dramatic impact on patients. Phil makes it a point to get out of his office and meet with other business units across the hospital's eighty plus sites in formal and informal interactions.

Checking in with colleagues and asking about their work has a number of benefits. First, it allows Phil and his team to keep up-to-date on business projects that require a security risk assessment – anything that involves health information or PII - but it also allows him to work as a

peer, not an adversary, or "security ogre". Phil says, "Business leaders understand risk. Our job is to present the security risks to them, and let them make decisions after reviewing all the information." Because Phil and his team have made an impression (via the meetings and networking), business leaders recognize the importance of preparedness and vigilance. As a result, they appreciate the merit of the risk assessments and weigh the results accordingly.

## AN ORGANIZATIONAL CHANGE MAKES A BIG IMPACT

It was not always so easy for the Information Assurance group to reach senior executives with their message and value. When Phil first joined Cooper University Health Care he reported to the CIO, a common organizational structure in hospitals. This meant that risk and security policy were delivered to business leaders through the lens of the technology organization. As a result, communication between the Information Assurance & Privacy Team and business units was limited. When the hospital made the decision to move Phil's team out of IT (they now are part of the Compliance department), the collaboration and direct interaction between Phil's team and other departments improved dramatically. "Because of that change, we communicate risk directly to business units. The move out of IT was among the biggest factors in the success of our information assurance and privacy program."

## SEPARATION OF SECURITY POLICY AND IT

"My role is to establish the standards and controls from an information perspective to maintain the confidentiality, availability, and privacy of our data. I am not a CSO. I do not handle security operations. My team focuses exclusively on governance, and not the technology used to enforce security policy. It can cause concern when the team responsible for maintaining the privacy and security of information is also the team responsible for bringing technology into the organization."

Gartner Agrees:

Today, only 38% of CISOs are outside of the IT department, but in their report, "Determining Whether a CISO Should Report Outside of IT", Gartner emphasizes a need to move CISOs out from under the CIO in the near term.

# Cloud Security

## Challenges & considerations for the modern organization

Gartner lists the top three concerns with cloud security as governance, cloud computing environments, and security and privacy. These concerns are prevalent due to the unchartered nature of the current cloud security posture within organizations, which results in a lack of control and oversight, along with a multitude of visibility challenges.

### Cloud security challenges and considerations:

- **Policies & Processes:** Put crucial policies into place so users may take advantage of the same cloud services that enable business growth without compromising security, compliance, and governance of corporate data.

- **Understanding Applications:** It is important to understand the specific workflow of applications that are running in the cloud. Ensure that you secure and monitor the data access to these apps, then enforce policies that correlate to all users.

- **Data Governance:** Recognize how your data is affected if a security event is detected and your data is seized for forensic analysis. It is important to understand the user access models when it comes to who is allowed to touch your data.

- **Data Encryption:** Understand how your data is encrypted (in transit or at rest), along with knowing where the encrypted keys reside and how the keys are protected.

- **Location of Data:** Be aware of the location of your cloud provider's data, considering how it may affect your information security policies and regulatory compliance mandates.

- **Data Classification:** Ensure you are able to perform your own data classification to enable appropriate user awareness and security levels for your sensitive data.


# LOS ANGELES WORLD AIRPORTS

## Achieving Control and Visibility with RSA Security Analytics, ECAT and Archer

### AT-A-GLANCE

**Challenges**

- Los Angeles World Airports needs to track everything that happens within its environment
- Working frequently with the FBI and the Secret Service, it has to be accountable for its cyber security
- Its goal is to have real-time detection of security events in order to ensure public safety
- Its SIEM did not give the IR team deep visibility into endpoint devices when responding to malware or APTs

**Results**

- RSA Security Analytics has enabled LAWA to greatly improve the speed of its response to immediate threats
- The solution enables deep-dive into payloads before and after a security event and delivers more information about each device than was previously possible
- The RSA Archer solution has also helped shorten incident response time as analysts can see all the information they need in one place, rather than spending time searching for it

**"My favorite thing about Security Analytics is the great forensics capability, that it can deep-dive into payloads before and after a security event. In addition, you get more information from the same device. For example, if you receive firewall logging information, you actually get more from Security Analytics than any other SIEM that I have."**

BOB CHEONG, CISO, LOS ANGELES WORLD AIRPORTS

Los Angeles World Airports

INGRAM MICRO

RSA

# Implementing the NIST Cybersecurity Framework

## Getting Started with NIST

Whether you currently implement the NIST Cybersecurity Framework in your organization or you are interested in adopting it into your security program, we are introducing resources (including the guide to the right), to help you understand and navigate this framework.

What is NIST? The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a risk-based approach to running a well-prepared and confident security program.

*"The framework provides a consensus description of what's needed for a comprehensive cybersecurity program"*

- Secretary of Commerce for Standards and Technology and NIST Director Patrick D. Gallagher

### Step 1. Align with business goals to gain executive sponsorship

Executive sponsorship is key to successfully implement the framework. Executive sponsorship leads to increased investment, improved visibility, and adoption of security efforts. To gain executive buy-in, security teams must demonstrate how they positively impact critical business goals related to revenue growth.

### Step 2. Identify risks related to revenue, strategy, and impact on core objectives

A thorough risk analysis helps identify areas of greatest concern and helps prioritize security objectives around the data and systems that are most critical to your organization.

### Step 3. Compare Current State of Security to Desired Risk Levels

It is important to create a baseline security profile, called a Target Profile, which outlines the current security posture as your starting point. You should also create a Target Profile that outlines where your organization should be in terms of security preparedness. With the two profiles, you will be able to map a program to transition from your current state to a more confident one via a risk management-based approach.

### Step 4. Continuously monitor, modify, and adapt

The most important aspect of any security program is its ability to react to changes, both internally and externally. It is vital to continuously monitor changes in business plans, processes, and procedures to identify and mitigate new risks as they arise.

# NIST

## ⊕ Framework for Improving Critical Infrastructure Cybersecurity

### WHAT IS THE NIST FRAMEWORK?

The Framework comprises a risk-based compilation of guidelines that can help organizations identify, implement, and improve cybersecurity practices, and creates a common language for internal and external communication of cybersecurity issues.

### FRAMEWORK CORE:

Set of cybersecurity activities, desired outcomes, and cybersecurity references that are applicable across all critical infrastructure sectors. This is the catalog of security activities that organizations should be considering if they want to effectively manage cybersecurity risk.

| FUNCTIONS | CATEGORIES | SUBCATEGORIES | INFORMATION RESOURCES |
|---|---|---|---|
| IDENTIFY | Asset Management | | |
| | Business Environment | | |
| | Governance | | |
| | Risk Assessment | | |
| | Risk Management | | |
| PROTECT | Access Control | | |
| | Awareness & Training | | |
| | Data Security | | |
| | Information Protection Processes and Procedures | | |
| | Protective Technology | | |
| DETECT | Anomalies and Events | | |
| | Security Continuous Monitoring | | |
| | Detection Processes | | |
| RESPOND | Communications | | |
| | Analysis | | |
| | Mitigation | | |
| | Improvements | | |
| RECOVER | Recovery Planning | | |
| | Improvements | | |
| | Communications | | |

### FRAMEWORK PROFILE

A Framework Profile is a selection of categories and subcategories from the Framework Core. The Profile component enables organizations to align and improve cybersecurity practices based on their individual business needs, tolerance for risk, and available resources.

1. As part of an initial base lining, organizations create a **Current Profile** by measuring their existing programs against the recommended practices in the Framework Core.
2. To identify a **Target Profile,** organizations employ the same Core criteria to determine the outcomes necessary to improve their cybersecurity posture.
3. Organizations should then compare the Current and Target Profiles to **identify the gaps** that should be closed to enhance cybersecurity and to develop and implement an action plan for addressing the gap.

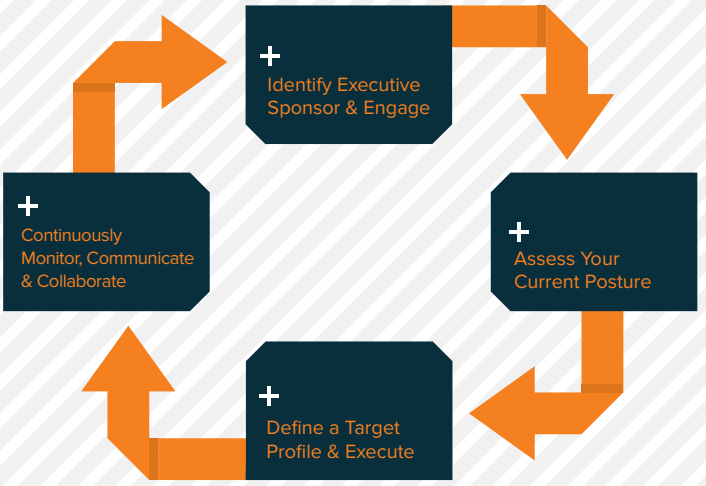
### FRAMEWORK IMPLEMENTATION TIERS

Implementation Tiers help create a context that enables organizations to understand how their current cybersecurity risk-management capabilities stack up against the characteristics described by the Framework.

| TIER 1 | TIER 2 | TIER 3 | TIER 4 |
|---|---|---|---|
| (Partial) | (Risk Informed) | (Repeatable) | (Adaptive) |

NIST recommends that organizations seeking to achieve an effective, defensible cybersecurity program progress to Tier 3 or Tier 4.

### TAKING ACTION TO IMPLEMENT THE FRAMEWORK




### CREATED BY:

KLogix

Request a poster-sized version:
marketing@klogixsecurity.com

# CYBER INSURANCE

## TIPS FROM AN EXPERT

According to the Department of Homeland Security, "A robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection". *(www.dhsg.gov)*

Christine Marciano
President, Cyber Data Risk Managers LLC

We asked Christine Marciano, the President of Cyber Data Risk Managers LLC, to provide some feedback on the current state of cyber insurance. Christine is a nationally recognized and experienced cyber insurance broker and thought leader. She has over 20 years of insurance experience and one of the few brokers who solely focuses on cyber.

**Best advice for a company with no cyber insurance policy in place:**

- Review your existing insurance coverage. Most insurance policies do not cover cyber, so it is important to explore stand-alone cyber policies.
- Make sure you align risks with the right coverages. You must ensure that there are policies and procedures in place and that you understand the type of vulnerability and risks you may face, to fully align with the correct coverage.
- Know what you are buying. It is vital that you understand exactly what is covered in your policy and that you review your needs as they relate to policy details.
- Know what is excluded. Many policies exclude things such as negligent computer security, so be fully aware of what your policy does not include. Seek out an experienced cyber insurance broker who can help you avoid these unnecessary exclusions.

### Process of Cyber Insurance

1. Establish policies and procedures. Most organizations utilize the NIST Cybersecurity Framework to gauge how they are protecting their data and how they understand the types of risks and vulnerabilities they may face. Important considerations include:

    a. Your understanding of cyber risk and vulnerability as they relate to the entire business.

    b. Your ability to demonstrate how you are protecting critical data.

    c. Your consideration of data breach scenarios.

2. Review types of coverages. Work with an expert to examine what types of coverage aligns with your specific cyber risks.

3. Underwriting application process. During this process, an expert will aid with appropriating specific coverages in order for an organization to obtain a policy that is customized to their specific needs.

### Future of Cyber Insurance

Christine believes that the product will differ greatly in the future. With revolutionary advances like the internet of things and driverless cars, risk will continue to drastically evolve. Policies will become more comprehensive and increasingly complex in the coming years as well. Eventually, a uniform framework, such as NIST, will be adopted in order to standardize the price of policies. As knowledge matures and policy pricing becomes more established, it will become a standard coverage and a clear priority for organizations.

# SANS CONTROL #13:
## Boundary Defense


**DAVE TASKER**

Senior Solutions Architect, addresses SANS Critical Control #13, Boundary Defense


Our team of security Solutions Architects continue to review each of the 20 SANS Critical Controls and provide advice for addressing each control in a typical enterprise organization.

Boundary Defense and its established tenets, like the use of firewalls to secure the perimeter, has evolved over the last decade. Today, attacks from outside the enterprise have a more communicative nature, usually spreading laterally once within an organization, and compromised or compromising devices often have direct access to the corporate network. A greater level of inspection and control needs to be applied to the boundaries that delineate areas of differing privilege.


The 13th SANS top critical control draws on the traditional principle of that DMZ, where access is controlled from untrusted to less trusted and less trusted to more trusted, then applies that across the enterprise on a least-privilege basis.


While often misconstrued as Internet-to-DMZ-to-Internal access architecture, the application of Boundary Defense is much broader. The 13th SANS top critical control draws on the traditional principle of that DMZ, where access is controlled from untrusted to less trusted and less trusted to more trusted, then applies that across the enterprise on a least-privilege basis. When properly applied, Boundary Defense employs varying levels of restriction in a number of ways.

First, it addresses the network by firewalling off mission critical systems and limiting access from internal and external sources based upon function and requirement; policy should restrict both inbound and outbound sessions.

Second, it leverages proxies and inline sandboxing appliances to detect and restrict the access and deployment of malicious software located outside the enterprise, and to intercede when currently compromised devices try to reach back to malware control mechanisms. Entry points, like client VPN connections, should grant restricted levels of access based upon role and should be supplemented with two-factor authentication to limit exposure. In a security-minded architecture, inbound, DMZ-initiated traffic should pass through an application proxy/firewall to further inspect and restrict traffic. Intrusion Detection and Intrusion Prevention also play key roles in identifying and blocking attacks, and utilizing a security analytics tool that can capture and record traffic for subsequent inspection can provide invaluable visibility.

Ultimately, Boundary Defense's goal is to determine and assign varying levels of trust and sensitivity to areas within an organization, and then safeguard the points at which those zones are traversed.

# Q & A with Maureen Medeiros

## IT Security Analyst Insurance industry

**1. What one skill should someone just starting out in security make sure they have? What can the industry do better to attract more young people to the profession?**

One skill the aspiring security practitioner should have is basic computer and networking skills. The user must be able to navigate around a PC and be able to run basic networking commands. A course in security and network fundamentals should be under their belt if they intend to get serious about the field.

The industry can reach out to the younger generation by attending career fairs, and by making security and hacking a big paying job.

**2. How do you train your end users to be security aware? Why do you think social engineering is so successful?**

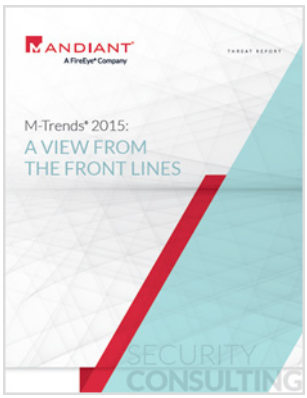
My organization currently utilizes web based training modules and our employees are required to take it annually. I believe Social Engineering is successful because it is human nature to trust, especially when it comes to friends and family. We automatically take their messages at face value, never considering that the email could be coming from a malicious source. What we need to do is change our behavior from trusting to suspicious, to protect ourselves from online predators, that is where training comes in.

I am a proponent of live interactive class room training. Engaging our internal customers and creating a curriculum that encourages role play is a great way to learn what not to do.

**3. Does your board view security as a cost center or enabler? If it is a cost center, what are you doing to change that perception?**

Security is most definitely viewed as a cost center. We do not generate revenue and are understaffed because of it. What management must realize is that we protect our corporate currency and our reputation, which is of equal or greater value. The last thing our board would want to see is our name on the front page of the Wall Street Journal. Conveying this message is difficult. Security tools and headcount is expensive but would be considered a good investment not if, but when we are exposed, which would lead our board to as the big question, “Why didn’t we protect ourselves?” It’s a vicious circle.

# Sponsorship message from FireEye




## A View from the Front Lines

This annual threat report provides key insights, statistics, and case studies illustrating how the tools and tactics of advanced persistent threat (APT) actors have evolved over the last year. The report also outlines approaches that organizations can take to improve the way they detect, respond to, and contain advanced attacks.

### M-Trends: A View from the Front Lines

Talking about the threat landscape is no substitute for experiencing it first-hand. “M-Trends 2015: A View from the Front Lines,” distills the insights gleaned from hundreds of Mandiant incident response investigations in more than 30 industry sectors. The report provides key insights, statistics, and case studies illustrating how the tools and tactics of advanced persistent threat (APT) actors have evolved over the last year. The report also outlines approaches that organizations can take to improve the way they detect, respond to, and contain advanced attacks.

Key findings include:

- Attackers had access to victims’ environments for 205 days before they were discovered.
- Sixty-nine percent of victims learn from a third party that they are compromised.
- Attribution is becoming harder as the lines blur between tactics used cyber criminals and nation-state actors.
- Over the last year, threat actors have used stealthy new tactics to move laterally and maintain a presence in victim environments.

**Download the report at www.fireeye.com**

**Download this report to learn:**

- How attackers are hijacking VPN and two-factor authentication
- Four steps to securing retail and other environments
- Five key questions your investigation should answer
- How the lines are blurring between nation-state attacks and cyber crime—and why it matters

**K logix**

1319 Beacon Street
Suite 1
Brookline, MA 02446

# FEATS OF STRENGTH

PROFILES IN SECURITY

VOLUME 3 / ISSUE 1

APRIL 2015

K logix