## Table of CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>What is the Current Nature of the Threat?</td>
<td>6</td>
</tr>
<tr>
<td>What is the Intent of the Threat?</td>
<td>7</td>
</tr>
<tr>
<td>Cold, Hard Cash is at The Heart of the Problem</td>
<td>7</td>
</tr>
<tr>
<td>The Crown Jewels: Intellectual Property and Secrets</td>
<td>7</td>
</tr>
<tr>
<td>Political Value</td>
<td>8</td>
</tr>
<tr>
<td>Threat Classes</td>
<td>8</td>
</tr>
<tr>
<td>How Is the Threat Behaving?</td>
<td>9</td>
</tr>
<tr>
<td>Incident Spotlight:</td>
<td></td>
</tr>
<tr>
<td>Sweeping Virus Attack on Manufacturer Highlights the Need for Security Basics</td>
<td>12</td>
</tr>
<tr>
<td>The Hard Truth</td>
<td>14</td>
</tr>
<tr>
<td>How Are Organizations Faring in Countering Cyber Threats?</td>
<td>14</td>
</tr>
<tr>
<td>It’s About Hygiene</td>
<td>15</td>
</tr>
<tr>
<td>Why the Struggle with Basics</td>
<td>15</td>
</tr>
<tr>
<td>The Industry Has Lost Focus</td>
<td>16</td>
</tr>
<tr>
<td>CISOs Rely Too Much on Technology</td>
<td>17</td>
</tr>
<tr>
<td>Compliance-Driven Security Is Not the Answer</td>
<td>17</td>
</tr>
<tr>
<td>Striking a Balance on Risk: Targeted Threats Versus Commodity Threats</td>
<td>17</td>
</tr>
<tr>
<td>Threat Spotlight: The Evolution of the Ransomware Risk</td>
<td>20</td>
</tr>
<tr>
<td>The Need for a Strategic Approach to Security</td>
<td>22</td>
</tr>
<tr>
<td>Five Focus Areas for Your Security Strategy</td>
<td>23</td>
</tr>
<tr>
<td>Risk Spotlight: How Trust in Third Parties Can Open the Door</td>
<td>24</td>
</tr>
<tr>
<td>How Can Organizations Protect Themselves?</td>
<td>28</td>
</tr>
<tr>
<td>Recommendations Based on H12016 Incident Response Engagements</td>
<td>28</td>
</tr>
<tr>
<td>Prevention Recommendations</td>
<td>29</td>
</tr>
<tr>
<td>Detection Recommendations</td>
<td>30</td>
</tr>
<tr>
<td>Response Recommendations</td>
<td>31</td>
</tr>
<tr>
<td>Conclusion: Return to the Basics to Strengthen Your Security Posture</td>
<td>32</td>
</tr>
<tr>
<td>Additional Recommended Resources</td>
<td>33</td>
</tr>
<tr>
<td>About SecureWorks</td>
<td>33</td>
</tr>
</tbody>
</table>
INTRODUCTION

With cybersecurity incidents in the news every day, every organization is giving at least some thought to what threats they may face and how well-protected they are. Organizations face several challenges when considering how best to protect themselves as the objectives and capabilities of threats continue to evolve.

When we set out to develop a report based on our 163 incident response client engagements over the course of the first half (H1) of 2016, we captured empirical data on types of threats, affected industries, and initial access vectors that threats use. However, we went back to the drawing board to ask ourselves, “What do organizations challenged by cyber threats and cyber risk actually need to know?” As a result, this report takes the form of an advisory aimed at jarring Security and C-Suite leaders just enough to evoke positive action and a recalibration of their approaches to security.

SecureWorks has unparalleled visibility into the threat landscape, with global Counter Threat Operations Centers monitoring over 4,300 organizations’ networks 24x7. Our incident response teams are reacting to security incidents every day, and a team of over 80 Counter Threat Unit™ (CTU) security researchers is constantly monitoring and evaluating the latest threat trends. Every day we see organizations fall victim to cyber incidents, and while some of these can require reasonably advanced controls to detect or prevent, the vast majority could often have been prevented through basic security best practices.
In this paper, we will examine:

- **What is the current nature of the threat?**
  What types of threats do we see today, and are they evolving or staying constant?

- **How are we seeing the threat behave?**
  What are the common attack vectors? While tactics can change over time, the fundamentals of cyber attacks haven’t changed. What are these fundamentals that we should protect against?

- **What is the “hard truth” our engagements illuminate?**
  Our observations on the security industry and how organizations like yours need to rethink core security processes and operations.

- **How can organizations protect themselves?**
  There are an overwhelming number of security controls and technologies available. Where are the most effective areas to focus your limited resources?

We will look at this from the perspective of tactical and strategic recommendations.

- **What are recommendations for improving security?**
  Understand the top security measures you can address to prevent, detect and respond to threats in today’s environment.

“**VICTIMS**” versus “**THREATS**”

We feel it’s very important to distinguish that this advisory is based on our many incident response and other engagements with organizations that fell victim to a cyber threat. This is a critical distinction. The focus on victims here means that we’re seeing firsthand what threats are having a very real impact. This also means that we get to observe what security operations — people, process and technology — organizations have in place and provide guidance that will actually resolve the issues these organizations face.
What is the **CURRENT NATURE** of the Threat?

Before considering what security controls an organization should focus on, it’s important to understand the threat.

Organizations face a range of threats, which can often be dependent on their line of business, status or the assets they are protecting. By understanding the types of threats that are likely to impact an organization, network defenders can define commensurate detection, prevention and response strategies, which form the foundation for a strong defensive strategy. However, based on hundreds of engagements serving the victims of cyber incidents, we found that most organizations are not cultivating a robust foundation.
Before considering what security controls an organization should focus on, it’s important to understand the threat — every type of threat has different tactics and intent. Here we try and outline the primary threats that we observe in the wild — who are they, and what are they trying to achieve?

What is the Intent of the Threat?

Organizations’ key assets do not tend to change significantly over time. SecureWorks typically observes threat actors demonstrate intent toward the following objectives, which organizations should consider when seeking to identify the threats they are facing.

Cold, Hard Cash is at The Heart of the Problem

Financially-motivated criminality is one of the main catalysts of cyber incidents that SecureWorks monitors, detects and responds to. There are a number of ways criminals make money through cyber means:

- **Financial theft from bank accounts.** Organized criminal groups seek to steal money from financial accounts. The majority of this activity involved indiscriminate attempts to gain access to a high number of accounts; however, some of these threat groups dedicate time and resources toward gaining access to and stealing from the bank accounts of specific wealthy individuals or organizations. Financial institutions are a natural target of this kind of activity, but all kinds of organizations are being affected in this way.

- **Financial information theft.** Threat actors seek to steal as many credit card details as possible, sell them on the black market or use them with a network of mules to make purchases that can be sold or cashed out.

- **Personal data theft.** There is a healthy black market in the sale of personal data. This data can be used in a variety of ways to make money, including fraudulently applying for loans, tax refund fraud, insurance claim fraud, etc.

- **Holding for ransom.** One of the most notable changes to the criminal threat landscape over the last two years has been the proliferation and evolution in the ransomware threat. Ransomware is malicious software that will encrypt files and data on a victim’s network, and only release the encryption keys upon payment of a ransom.

- **Theft of computing power (botnets).** — Organized crime groups often try to surreptitiously take control of as many unsuspecting systems as possible, so that they can sell access to the computing power on the black market for malicious acts such as sending spam and DDoS attacks.

The Crown Jewels: Intellectual Property and Secrets

Organizations that hold information that can be leveraged for competitive advantage, such as manufacturers, pharmaceutical companies and defense companies, are typically of interest to organizations who want to short-circuit their own R&D, either for political, economic or financial
advantage. This can involve unscrupulous competitors or nation states.

### Political Value

Some organizations’ data and infrastructure can be leveraged for political advantage or to make a political statement. Examples of this are bulk theft of foreign PII data by a nation state to support their domestic counter-intelligence investigations, or a retaliatory destructive act from a nation state against an overseas media organization (e.g., North Korea’s high-profile acts directed at Sony Pictures).

### Threat Classes

We see different groups seeking to achieve one or more of the objectives listed in the chart above.

<table>
<thead>
<tr>
<th>Class of Threat</th>
<th>Objectives</th>
<th>Common Tactics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacktivist</td>
<td>- Deface, disrupt, or destroy systems for political or ideological purposes.</td>
<td>Scan and exploit of externally facing systems.</td>
</tr>
<tr>
<td>Nation State</td>
<td>- Information theft/espionage for political, economic or military gain. - Destruction or disruption of systems for political, economic or military gain</td>
<td>Targeted attacks, that often use a range of methods and tools, escalating to zero-day vulnerabilities and advanced malware if required.</td>
</tr>
<tr>
<td>Insider</td>
<td>- Theft of information or abuse of systems for financial gain, personal gain or in pursuit of revenge.</td>
<td>Abuse of existing employee access to access data or manipulate systems.</td>
</tr>
<tr>
<td>Cybercriminal</td>
<td>- Theft of capital. - Theft of large volumes of data (personal or financial) for sale on black market. - Hold information to ransom</td>
<td>Commoditized, untargeted malware typically delivered by publicly disclosed vulnerabilities.</td>
</tr>
</tbody>
</table>

Organizations struggle to defend against high volume, financially-motivated cybercriminals. In H1 2016, 82 percent of IR engagements were in response to financially-motivated cybercriminals (see Figure 3).

We see both untargeted and targeted activity from this class of threat actors; however a majority of these threats appear to be untargeted. Our incident responders observed a large quantity of commodity threat activity, such as a watering hole attack. This is minimal work for threat actors, as they are not required to research a victim, but rather place bait and wait for unsuspecting victims to bite. The most significant cybercrime threat was ransomware incidents, which made up 30 percent of all activity. Ransomware is a tried and true attack mechanism for hackers.
today. It provides threat actors a straightforward and direct revenue stream and does not require infrastructure maintenance. There is no indication that a single industry vertical is being targeted with ransomware; rather, it is industry agnostic.

How Is the Threat Behaving?

The proliferation of cyber incidents across companies, industries and geographies makes cybersecurity challenging for network defenders. However, the reality is that the majority of adversaries are still finding success through well-known methods and techniques.

Most cyber incidents can be broken down into two phases: they first get in the network, and then they move around and try and achieve their objectives. When we look at the primary methods we see attackers use to get into networks, we can start to make the security challenges associated with these methods manageable:

- **Compromise of vulnerable public-facing systems**: Web applications, remote access solutions and other Internet-facing systems may have vulnerabilities in them that allow an attacker to gain privileged access to a system, giving them a foothold on the network.

- **Legitimate credentials are compromised**: A username and password is disclosed, allowing the attacker to freely access systems and move around the network. These may be compromised through a previous malware attack (keyloggers), brute forcing vulnerable systems, stolen from a third-party breach and reused somewhere else or captured via a phishing attack.

**Figure 3**: Summary of threats during SecureWorks IR engagements between January and June 2016.
Note: Sixteen percent of engagements did not have sufficient information and logging to establish how the adversary got in. This was removed from the data set shown above.

**Figure 4**

SOURCE: SecureWorks aggregated data from Incident Response client engagements in H1 2016
• **Malware is delivered in an email:** A user may open malicious software attached to an email. This could be a highly targeted spear-phishing email from someone they think they know, or an untargeted opportunistic spam email. This then gives the attacker control over the infected system, to steal credentials and/or move around the network.

• **Malware is downloaded from a website:** A user may unintentionally access malicious software hosted on a website. This could be a malicious website, or a legitimate website that has been compromised to deliver malware.

• **Third-party compromise:** A third party — maybe a supplier or partner — can be compromised using one of the methods above, potentially giving them access to your information, systems or infrastructure.

When SecureWorks compiled the data from our incident response engagements in the first half of 2016, we found that 38 percent of adversaries were leveraging phishing to initially gain a foothold in victims’ environments, making it the dominant choice. Although not a new and glamorous technique, phishing is highly effective; this is why we continue to see its rampant use. From the perspective of an attacker, “If it ain’t broke, don’t fix it.”

Scan and exploit was the second highest access vector at 22 percent, followed closely by web exploits at 21 percent. Internet-facing infrastructure is exposed to high and low capability threats, which can lead to navigating a field of landmines if your organization is not patching appropriately. Keeping up with patching can be cumbersome; however, it is critical to prioritize anything that is Internet facing.

These are key activities that any organization’s cyber-defense should be focused on preventing. When we consider the number of technology controls we have available to do that, it often feels like we may be overcomplicating the picture. SecureWorks’ overwhelming volume of recommendations to customers following a security incident relate to basic security hygiene.

Phishing is highly effective; this is why we continue to see its rampant use. From the perspective of an attacker, “If it ain’t broke, don’t fix it.”
Sweeping Virus Attack on Manufacturer Highlights the Need for Security Basics

The Situation
A large-scale manufacturing company reached out to the SecureWorks Incident Response team with a big problem: a mass of disparate viral infections had penetrated its defenses and were not being prevented by the organizations antivirus solution. Antivirus alerts were being generated continuously and the infections were spreading rapidly across the network.

Without resolution, the risk of downtime could cost tens of thousands of dollars.

The Nature of the Threat
When the client’s antivirus solution continued to create alerts for new computers being infected, its security team was challenged to identify the cause of the infection.

The antivirus tool—while able to generate alerts—lacked the ability to stop the spread of the infections.

The manufacturer attempted to fix the problem internally and requested help from its IT outsourcer and its antivirus provider. The initial effort was aimed at deploying custom antivirus definition files. Four days passed and the infection only got worse, so they reached out to SecureWorks.

Our Incident Response team assessed the nature of the attack and realized the client was dealing with an unremitting, self-replicating worm named “Kwampirs.” The initial infection was never discovered. However, once the malware was introduced into the environment, it executed through the rights of a network administrator with access.
to most of the organization’s endpoints — laptops, desktops and servers. As a result, the malware spread to thousands of endpoints within the network (more than 50 percent of total endpoints), increasing the organization’s concern for both information security and the impact on system availability and performance.

SecureWorks deployed proprietary tools and instrumentation to monitor the environment and quickly noticed other unrelated infections spanning both targeted and commoditized attacks that had gone undetected previously, including:

- Banking Trojans
- Bitcoin mining malware
- Remote access Trojans sent to C-level executives

**Lessons Learned**

We identified three major oversights that created vulnerability gaps a threat actor was able to exploit:

- Many users had uncontrolled administrative privileges
- A large number of servers were running on Windows XP, which is no longer vendor-supported
- Limited incident response processes and capabilities to respond to an attack

All of these oversights had to do with the fundamental security hygiene in place. Two of the three missteps are people and process issues. In this case, getting the basics of security right eliminates a significant portion of the attack surface and potential vulnerabilities from the beginning and is not expensive to implement.

Bringing in the right expertise and tools to effectively respond to this security incident allowed the client to gain visibility of, and respond effectively to, other unidentified threats. The client developed a better understanding that, even with security technology, an insufficient emphasis on security fundamentals had left its network exposed and vulnerable. A plan to address security fundamentals will help this manufacturing company manage risk much more effectively in the future.

**Important note:** You may be thinking that this example couldn’t happen to your organization. This example was selected because it’s representative of the practices we see across many organizations today.
The Hard TRUTH

Covering basic health and hygiene in cybersecurity is a multi-layered process.

How Are Organizations Faring in Countering Cyber Threats?

Jeff Carpenter, Director of SecureWorks’ Incident Response and Digital Forensics practice, says that he’s always being asked if organizations are getting better at security. Based on our response engagements in H1 2016, he says, “We’re getting better at learning how badly we’re losing.”

But how is that possible when there is more awareness, emphasis and investment in cybersecurity by organizations than ever before? It didn’t take long for our experts to cut to the chase of what they see as the problem and what they see as the solution to address cyber threats and risk more effectively by organizations.
It’s About Hygiene

When asked what he thinks organizations should be aware of in regard to cybersecurity, Don Smith, Director of the Counter Threat Unit™ (CTU) Cyber Intelligence Cell at SecureWorks, says, “Basic health and hygiene across the IT estate is still something that most organizations fail at. For example, we still find people who don’t use multi-factor authentication for VPN or email.”

Covering basic health and hygiene in cybersecurity is a multi-layered process. It means knowing your assets, the information contained in them, the controls and perimeter and evaluating user access and privileges to help minimize the risk of user error and remote threat activity.

The cyber threats we’ve resolved for clients in H1 2016 make the case for getting the basics right, and we believe implementing effective processes at the core of your security operations to enable prevention, detection, response and prediction is the foundation for a strong defense. However, based on hundreds of engagements serving the victims of attacks, most organizations are not cultivating that robust foundation.

On the flip side, we’ve seen first-hand examples where organizations with strong security foundations in place were more effective in countering and resolving incidents before significant damage could be done. Take, for example, an organization we worked with that had 130 ransomware phishing emails get into its environment. Though a user clicked on the link contained in the email activating the ransomware to start encrypting files, the ransomware was unable to spread. This was possible because the security team was able to minimize user access and permissions.

Additionally, because the organization had a comprehensive backup strategy in place, what little data that was encrypted could be easily recovered. Instead of a crisis, the attack merely created an exercise in removal of the malware from the environment. The organization’s hygiene practices saved the security leader from having a very difficult conversation with the CEO.

Why the Struggle with Basics?

We see a number of potential explanations—both internal and external—as to why most organizations struggle to build a strong security foundation based on people, process and technology. At the core of several of these explanations is what we see as an over-reliance on technology:

- Vendors are failing to act as trusted advisors and continue to make promises that their products can’t fulfill, minimizing the value of the investment.
- CISOs are counseled to focus on the latest security technology rather than address the basics of people and process.

“Basic health across the IT estate is still something that most organizations fail at.”

— Don Smith
Director of CTU Cyber Intelligence Cell
SecureWorks
• A compliance-first approach has blurred the reality that security is the path to compliance.
• Organizations are focused on less-likely targeted threats when they are still incapable of defending against the many commodity threats hitting their perimeters every day.

The Industry Has Lost Focus

In essence, the industry has not served the best interests of the organizations it promised to protect. Somewhere along the way—as is true in many other industries—serving customers simply became about selling more products.

The industry, for its part, has insisted that if organizations kept adding technology that they’d achieve strong security postures. But none of the layers were ever removed, and the supporting resources to implement processes to tune, monitor and action the output of those technologies was often absent.

The results can be complex security technology stacks that are ineffective at holistically addressing the threats organizations face. Where it once was stressed that technology was the answer, it has become apparent that through this orientation, organizations have lost the intensity of their focus on the fundamentals that offer genuine support for their security goals.

Don Smith, Director of CTU Cyber Intelligence Cell at SecureWorks, puts it this way: “It is rarely the case that we come across an incident and we think, ‘The client could have done more by investing in a new piece of security technology.’”

The trusted advisor must:
• Keep organizations apprised of the changing nature of the threat landscape and how it may introduce risk specific to your organization.
• Help organizations solve their broader security challenges or achieve their desired outcomes. This includes being able to articulate and demonstrate the efficacy and value of their solutions in reducing risk.
• Understand your organization and its priorities.
• Provide honest feedback and guidance, unfettered by specific product, service or solution bias, on how security and C-suite leaders can secure their sensitive data, their employees and the overall health and reputation of their organizations.
• Help organizations optimize and enhance their existing security investments.

Ask yourself, “Are the security providers we’re working with acting as trusted advisors?”

—Don Smith
Director of CTU Cyber Intelligence Cell at SecureWorks
and we think, ‘The client could have done more by investing in a new piece of security technology.’

Expanding further, Jeff Carpenter adds, ‘But that doesn’t mean the problems discovered are being fixed. Organizations are spending hundreds of thousands of dollars on security platforms and services, but that doesn’t mean they’re making it more difficult for the adversary.’

The security industry-at-large is contributing to the over-reliance on technology while also not providing sufficient validation or proof of the efficacy of those technology solutions.

CISOs Rely Too Much on Technology

The pressure to keep up with the latest security technology has been problematic for Chief Information Security Officers (CISOs). Once a technical role, the CISO now has more of a business role. Every day, SecureWorks experts engage with CISOs working at companies across many industries, sizes, geographies and markets. Most of them fall into two camps — the technical CISO, who grew up through the ranks of the IT department, and the business risk-focused CISO who grew up in a risk and compliance department. Learning to balance both can be challenging for even the most seasoned leaders.

The result is that security technology vendors have had it pretty easy— IT-focused CISOs who are used to using technology naturally look to security technologies to solve problems, and risk-focused CISOs rely on technology vendors to educate them on what they need to protect their organization.

Compliance-Driven Security Is Not the Answer

Letting compliance mandates propel your approach to security is no panacea either, and the industry is still struggling to move away from it. Case in point: we’ve talked to security teams at financial institutions that are spending as much as 40 percent of security staff time on compliance initiatives rather than security initiatives that matter to their organizations. Compliance is often seen as a catch-22: organizations believe that the choice is between compliance and security, with compliance often winning out because revenue could be put at risk.

The irony is that a strong emphasis on security will consequently address most compliance aspects, while taking a compliance-first approach often leads to gaps and vulnerabilities as security teams are distracted from managing genuine threats and risks.

Striking a Balance on Risk: Targeted Threats Versus Commodity Threats

We believe many organizations are placing undue emphasis and resources on combatting advanced threats, when commodity threats present a greater likelihood of attack and associated risk.

Based on our 163 response engagements we performed in H1 2016, only 12 percent involved a targeted threat (Figure 1).

**Figure 1**

<table>
<thead>
<tr>
<th>TYPE OF THREAT</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targeted</td>
<td>12%</td>
</tr>
<tr>
<td>Opportunistic</td>
<td>88%</td>
</tr>
</tbody>
</table>

Q1/Q2 2016

SOURCE: SecureWorks aggregated data from Incident Response client engagements in H1 2016
Defining the Target

Targeted Threats: SecureWorks CTU researchers define a “targeted threat” as an attack perpetrated by an adversary whose intent is specific to an organization. In this case, the actor, through their persistence, is able and willing to use multiple methods to achieve their aim.

Commodity Threats: Commodity, or opportunistic, threats are defined as any activity whereby the adversary does not act with high intent against a target or select group of targets. Actors behind commodity threats are more likely to deploy a single method of compromise against a larger number of targets, consequently requiring an individual organization’s team to expend less effort and resources to investigate, contain and evict.

According to Jeff Carpenter, Director of SecureWorks’ Incident Response and Digital Forensics practice, “Most organizations should stop worrying about zero-day attacks, when there are so many other threats that are much more prevalent. It’s like running across a road to escape from a possible stalker, but neglecting to look for oncoming vehicles.”

That is not to say some organizations or industries should not be focused on the problem posed by targeted threats. They absolutely should be. Take, for instance, the chart on the right breaking out the industries targeted most based on engagements.
Manufacturing organizations represented the largest share of incidents involving targeted threats at 30 percent (Figure 2), which could indicate threat actors seeking economic intelligence. Any new product, process or technology a manufacturer creates could be a prime target for hackers to steal. Healthcare, on the other hand, although in the headlines for ransomware, does not tend to attract targeted threats. In fact, only five percent of the targeted organizations we assisted in H1 2016 were in the healthcare industry.

Security leaders must reassess their risk from targeted attacks versus more common, commoditized threats and reprioritize resources as appropriate. There is no sense in focusing on targeted threats unless organizations have the security fundamentals in place to protect against commodity threats.

"Most organizations should stop worrying about zero-day attacks, when there are so many other threats that are much more prevalent."

— Jeff Carpenter, Director of SecureWorks’ Incident Response and Digital Forensics practice
The Evolution of the Ransomware Risk

Your Money or Your Data
Ransomware is a pervasive security threat that is impacting organizations across all sectors. Between 2015 and 2016, SecureWorks saw a 75 percent increase in the average number of incidents per month that we responded to that involved ransomware. Estimates from the FBI put ransomware on pace to be a billion dollar source of income for cybercriminals this year.¹

Nature of the Threat
The ransomware threat landscape is rapidly evolving; it presents a low barrier to entry for threat actors and has the potential to offer high rewards.

In addition to the apparent increase in scale, the number of ransomware variants is rising exponentially. “Ransomware is evolving into campaign-oriented toolsets that are used for a period of time and then tail off. We see ransomware families that come and go within six to eight weeks,” according to Don Smith, Director of CTU Cyber Intelligence Cell at SecureWorks.

Lessons Learned
We are seeing no indication that any single industry vertical is being specifically targeted by ransomware. As an industry agnostic threat, all organizations should prioritize strategies for the prevention of and response to ransomware events. Based on the lessons identified during recent incident response scenarios, actions such as rights minimization, response planning, user education and frequent, segregated backups would have had the most significant defensive impact.

Ransomware is a form of malware that targets organizations and individuals in an effort to deny the availability of critical data and systems. When the victim is no longer able to access their data, the cyber-actor demands the payment of a ransom — usually in Bitcoins. The cyber-actor then provides an avenue — such as decryption keys — for the victim to access their encrypted data.
The Need for a STRATEGIC APPROACH to Security

Many organizations lack a unified vision or plan for how they address security into the future.

A security strategy should include the following characteristics:

- **Risk based**: Your strategy must be based on the risks you have identified.
- **Pragmatic**: Actions are prioritized and controls are implemented that reduce the greatest identified risk first.
- **Be driven by security, not compliance**: Compliance will naturally follow from good security, but the opposite is not true.
- **People and process before technology**: Focus on what people do, rather than the tools and technology. Tools and technology play a supporting role.

Our observations are that many of the organizations we have assisted in responding to an incident lack a comprehensive security strategy. Most have lots of activities or ongoing projects to address aspects of security, but lack a unified vision or plan for how they address security into the future. But this needn’t be true for your organization.

By focusing on the five areas on the next page, the ability to reduce substantial risk for your organization is entirely within your control and largely within your available resources. Focus on hygiene and security basics first. Get involved in every initiative that touches sensitive data from the start. And test your incident response plan to increase your organization’s confidence in its ability to respond to an incident and get back to normal operations quickly.
Five Focus Areas for Your Security Strategy

1. **Understand the extended enterprise.** You need to establish a full picture of what you’re trying to protect. And remember that it’s no longer defined by a perimeter — your suppliers, partners and technology providers may all have access to your data. Take a data-centric approach by defining your key assets and knowing where they reside (e.g., internally, shared with third parties, in the cloud, etc.). Then understand who has access and which systems support them. By understanding the systems, controls and access levels, you’ll have a picture of the risk landscape.

2. **Increase visibility.** Once you understand your risk landscape and where your vulnerabilities are, you can prioritize investments and controls. By collecting and monitoring all of your security events, you’ll have the capacity to quickly detect incidents that might otherwise go unnoticed. Employ host and network-based IDS/IPS to inspect user activity to prevent malicious acts and identify trends over time within the infrastructure. Remember that it is important to share visibility with the C-suite, board and your security team. Running vulnerability scans, conducting penetration tests and ensuring patch and configuration management are current all contribute to risk reduction on internal infrastructure.

3. **Build a culture of security.** This is inarguably the biggest task for a CISO. It means transferring and converting mindsets within the organization from thinking that security is an IT job to understanding that it is a shared job across the organization. Everyone within the organization must take responsibility for their role in protecting information. Security is not just an IT problem, but a business risk. Invite people from finance, legal, HR and other areas of the company into forums to discuss security and help sell it to the rest of the business. Governance is critical to driving this cultural change.

4. **Train your users.** The #1 risk that organizations face in security is actions taken by employees—whether intentional or through not knowing or caring about what they do. Training is important enough to be considered a major focus area for your security strategy. A large proportion of the intrusion attempts we see come via phishing and social engineering. This means that your employees are the targets. They need to very clearly understand what this means and what to do.

   Consider layered training that is computer based (with quizzes), coupled with face-to-face training with key individuals through workshops, webinars or lunch and learn events. Basic training is about security essentials and should be based on roles. An example is training a customer service representative how to collect sensitive information from customers over the phone in the call center. Your senior executives also carry a lot of risk given the sensitivity of the information they have access to and the ability for attackers to target them specifically.

5. **Be prepared to respond to incidents.** Gartner predicts that 60 percent of security budgets will be spent on detection and response by 2020. Starting now to build a tried and tested incident response process will serve you well. Formalize roles and responsibilities in every type of incident so that people understand what is required of them. Know exactly where your logs are and how to gain access to them. For example, with moves to the cloud, critical logs could reside with third parties. Make sure to test your response plan to ensure that organizational boundaries won’t get in the way and establish access to specialist incident responders so that they’re available to help, should you need them.

Again, it is important to reiterate that we believe that security leaders, with the support of their executive leadership and the Board of Directors, have much more control over cyber risk as a result of strong internal processes and robust hygiene than currently realized. This control is becoming especially important in relation to the increasing risk posed by third parties.

---

How Trust in Third Parties Can Open the Door

Breaking In Through the Side Door

When a targeted threat group runs into an obstacle trying to enter a victim’s network, they will often switch gears and try a new tactic. If they can’t enter through the front door, they will try the side door, meaning they will compromise third parties as a means to gain access to well-defended networks.

One of SecureWorks’ clients was recently compromised by an advanced, targeted threat group. The manufacturer had a strong perimeter defense with malware sandboxing, IDS/IPS, above average logging and firewalls with both ingress/egress filtering. They also had nascent endpoint monitoring and had taken precautions when segmenting their network by segregating critical assets onto two separate domains — A and B. What they did not have, however, was knowledge of how one of their partners had opened them up to attack.

Nature of the Threat

Through reconnaissance, the threat actor determined that the intellectual property they were after was on Domain B, and that a third party providing help desk services for the targeted organization had access to Domain A. This was the threat actor’s golden ticket. SecureWorks’ targeted threat hunters determined the threat actor was in the third party’s environment for 11 days before they gained access to the targeted organization’s network.
Domain A. By compromising the third-party network, they were able to leverage the partner’s legitimate connectivity to the organization they wanted to attack.

To pivot from Domain A to Domain B, the threat group gained access to several administrator accounts and used them to access Citrix servers in Domain A. The threat actor then leveraged access to these Citrix servers to harvest additional credentials, this time for systems in Domain B. Once in the targeted part of the network, the threat group had created multiple web shells in Domain B and also created an OWA\Auth directory on two exchange servers. This triggered IPS/IDS alerts for webshell activity and also was caught with SecureWorks’ RedCloak solution.

Lessons Learned
This is a useful example of the importance of securing endpoints, which proved crucial to identifying the nature and scope of the threat activity in the network. However, in this case it is important to acknowledge that the ability of the organization and SecureWorks’ threat hunters to respond to alerting (people and processes) were just as important as the implementation of endpoint security tools (technology).

About a week and a half after the client evicted the threat actor from their environment, the adversary successfully re-entered the same third-party network. However, because both the network bridge and domain trust had been removed from the targeted organization’s network, the adversary was unable to repeat the same intrusion steps to reach Domain B. From this incident, the targeted organization also learned about the importance of continuously managing third-party security risks and gaining security assurances from its partners.

In a recent Ponemon study, 73 percent of respondents see the number of cybersecurity incidents involving vendors increasing. 2 Securing your organization’s borders alone is no longer sufficient; your vulnerabilities now extend to the ends of your partners’ networks.

According to a 2016 study conducted by Bomgar, on average, 89 third-party vendors are accessing company’s networks every week. 3

With each new vendor connecting to your network and data, another channel is opened for adversaries to take advantage.

With third-party breaches on the rise, businesses are faced with organizational challenges that require cultural changes, security prioritization and internal restructuring. Our observations suggest three situations must be addressed for improved security when working with third parties:

• Organizations put too much trust in their partners or affiliates’ security operations.

While your organization is managing all of the required security controls, you can’t assume that third-party partners or affiliates are doing the same. Bomgar found that an astonishing 92 percent of respondents say they trust their vendors completely or most of the time, with 67 percent

---

2 Ponemon Institute, Data Risk in the Third-Party Ecosystem, April 2016

admitting they believe they tend to trust vendors too much.1 With the rise of breaches attributed to third parties, organizations need to start focusing on the selection and governance of these partnerships, rather than blindly trusting their partners’ security controls. Developing focused and structured relationships will help manage these risks.

• No clear accountability for third-party risk management. According to the study administered by Ponemon, 21 percent of respondents said there was no one person/department accountable for handling of a third-party risk management program.4 The remainder of the responses were across the board, which included: Head of procurement, CISO, CIO, General Counsel/Compliance Officer, Chief Risk Officer (CRO) and Chief Security Officer (CSO). The variety of departments with responsibility indicates that there is no standardized program for third-party vendor management.

Regardless of who is assigned ownership—and someone should be—we recommend that it become a standard practice to include oversight and guidance from the security leader to help minimize the unforeseen security risks associated with vendors.

• Security is not the top concern when selecting the vendor to work with.

Lastly, when selecting third-party vendors, many times cost and functionality drive the selection process rather than their security score-card. In the Vendor Vulnerability Study, 74 percent of respondents believed that vendor selection overlooks key risks.5 Quantifying the risks of a partner before onboarding them is an essential piece in maintaining your security posture. A third-party risk assessment enables you to manage risk associated with each vendor based on your company’s policies and procedures.


74% of respondents believed that vendor selection overlooks key risks.5
“With the rise of breaches attributed to third parties, organizations need to start focusing on the selection and governance of these partnerships, rather than blindly trusting their partners’ security controls.”
How Can Organizations PROTECT THEMSELVES?

The key pillars your security strategy should consider

Improving security requires a combination of bottom-up action and top-down thinking. While CISOs should build and communicate a strategy that moves their security function in the right direction, equal focus must be given to the more tactical recommendations that we make time and time again when helping customers who have been breached. In this section, we will first look at some of those tactical recommendations and then outline the key pillars your security strategy should consider.

Recommendations Based on H1 2016 Incident Response Engagements

SecureWorks provides comprehensive recommendations to affected organizations after all incident response (IR) engagements to help organizations understand where they can improve and what defensive actions to prioritize. Below are aggregated findings from 163 Incident Response client engagements from the first half of 2016.
### PREVENTION RECOMMENDATIONS

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improve Regularity of Software Updates/Patching</td>
<td>High</td>
</tr>
<tr>
<td>Manage User Account Privileges</td>
<td>High</td>
</tr>
<tr>
<td>Implement Web Application Firewall or Web Content Filtering</td>
<td>High</td>
</tr>
<tr>
<td>Implement Two-Factor Authentication (2FA)</td>
<td>High</td>
</tr>
<tr>
<td>Implement Robust Password Policy</td>
<td>High</td>
</tr>
<tr>
<td>User Education</td>
<td>High</td>
</tr>
<tr>
<td>Vulnerability/Penetration Test Network</td>
<td>High</td>
</tr>
<tr>
<td>Implement/Configure Application Whitelisting</td>
<td>Medium</td>
</tr>
<tr>
<td>Implement Application Whitelisting</td>
<td>Medium</td>
</tr>
<tr>
<td>Restrict Use of Uncommon Protocols</td>
<td>Medium</td>
</tr>
<tr>
<td>Resolve Network Architecture Issue</td>
<td>Medium</td>
</tr>
<tr>
<td>Reconfigure Internet-Facing Services</td>
<td>Medium</td>
</tr>
<tr>
<td>Configure Existing Security Controls</td>
<td>Medium</td>
</tr>
<tr>
<td>Block High-Risk Email Attachment Formats</td>
<td>Medium</td>
</tr>
<tr>
<td>Apply Threat Intelligence to Security Controls</td>
<td>Medium</td>
</tr>
</tbody>
</table>

**Source:** SecureWorks aggregated recommendations based off Incident Response engagements in H1 2016

---

### Prevention Recommendations

The top recommendation we provided clients, and therefore one of the main contributing factors to help prevent cyber incidents, was to improve the regularity of software updates and patching. Keeping up with the latest software updates and new patch releases can be overwhelming. However, having an effective patch management process is a critical component to help prevent potential cyber threats. Prioritizing patching based on critical assets and Internet-facing systems is a sound starting point for addressing this issue.

Additional recommendations to focus on when prioritizing patching include:

- Implement a systematic, accountable and documented process for managing exposure to vulnerabilities through the timely deployment of patches
- Ensure vulnerability managers are adequately resourced and any barriers to patching delivery are minimized
- Test the effectiveness of your patching program while measuring and tracking the results
Detection Recommendations

As stated earlier in the advisory, SecureWorks’ top detection recommendation for organizations was to implement an endpoint security solution. An endpoint security solution should provide 24x7 visibility into the activities taking place on all endpoints. Real-time, continuous monitoring allows you to detect potential malicious activity and provide endpoint forensics that will help investigators—whether internal staff or third party—determine how an attack unfolded if a breach is detected.

An endpoint threat detection solution must:

- Detect malware and other tradecraft a threat actor may use, as well as detect behaviors suggesting their presence in your environment.
- Help reduce the response and detection time for attacks and lower the effort and cost to fix them.
- Provide your organization greater context into the motives and identities of attackers, so new threats by them and others like them can be prevented.
Response Recommendations

The most common recommendation we provided clients in regards to responding to threats was to enhance their logging capabilities (including enhancements to log retention and verbosity). However, it is important to note that our three top recommendations rely more on people and process than on state-of-the-art technology.

Logs are a valuable source of information during the incident response process. Log management gives insight into the activity on systems and applications which can help determine the appropriate anatomy of a cyber attack and its impact with a higher degree of certainty. If your access to logs is limited, or if logs are missing, incident responders are disadvantaged when attempting to understand how the incident occurred and what the organization could have done differently.

**SecureWorks recommends that organizations should:**

- Ensure full and complete log collections are retained and available for critical business systems.
- Know how long the logs are stored before they are overwritten. Understand the verbosity of logging levels to make sure the appropriate information is being logged to support incident response and forensic investigation.

- Maintain logs on the following systems at a minimum: Firewalls, IDS/IPS, DNS, VPN, Active Directory, Critical Servers/Systems and Web Services. These logs should be retained for 13 months as a best practice.
Conclusion
RETURN TO THE BASICS
to Strengthen Your Security Posture

Focus on security fundamentals to safeguard your people, sensitive data and business operations

Threat actors continue to use tried and proven methods of attack and successfully exploit businesses that fail to focus on the fundamentals of hygiene in their security programs. This is true across all industries. It’s time to take a step back and realize that industry and security teams need to recalibrate their emphasis on technologies to focus on achieving measurable results and outcomes or solving broader business risk challenges for organizations.

It should now be apparent that regaining a focus on security fundamentals will support the goal of cybersecurity: to safeguard your people, sensitive data and business operations.

Don’t be satisfied with bold promises and Band-Aids to security problems offered by vendors. CISOs who demand outcomes—true solutions to security problems—should expect to see their vendors step up into the role of trusted advisors. With a strategic partnership, organizations will be prepared for and competent at detecting, preventing and responding to the most persistent and creative attacks deployed by threat actors.

Ask for help to achieve outcomes and results from your security vendors — and demand to see proof.
It should now be apparent that regaining a focus on security fundamentals will support the goal of cybersecurity: to safeguard your people, sensitive data and business operations.

Additional Recommended Resources

- 2016 Underground Hacker Marketplace Report
- Communicating with the Board of Directors: IT Security Leaders Roundtable
- Board Oversight of Cybersecurity Risk: A Framework for Inquiry
- Community Building Is Essential to Hackers—and Directors

About SecureWorks

SecureWorks is a world-leading provider of world-class information security solutions with more than 4,300 clients in 58 countries. Organizations of all sizes rely on SecureWorks to protect their assets, improve their compliance and reduce their costs. Our combination of award-winning security expertise and client support makes SecureWorks the premier provider of information security solutions.
SecureWorks is a global provider of intelligence-driven information security solutions exclusively focused on protecting its clients from cyberattacks. SecureWorks’ solutions enable organizations to fortify their cyber defenses to prevent security breaches, detect malicious activity in real time, prioritize and respond rapidly to security breaches and predict emerging threats.

Corporate Headquarters
1 Concourse Pkwy NE #500
Atlanta, GA 30328
1.877.838.7947
www.secureworks.com

Europe & Middle East
France
8 avenue du Stade de France
93218 Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center, Unterschweinsteige 10
60549 Frankfurt am Main
Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
UK House, 180 Oxford St
London W1D 1NN
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111
00971 4 420 7000

Asia Pacific
Australia
Building 3, 14 Aquatic Drive
Frenchs Forest, Sydney NSW
Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp