DIY is DOA: Cybersecurity Moves Toward Hybrid Models
Information security always was complex and technically challenging. But the increasing borderlessness of cloud- and mobile-enabled organizations in the last 15 years has exponentially multiplied that challenge.

More recently, what’s at stake has risen dramatically as very public cybersecurity breaches have damaged the reputation of trusted brands that possess our personal information. CIOs, CISOs and CEOs are being fired; board members are being sued.

Security professionals are caught in the middle. Their jobs continuously get harder, demanding a broad range of highly specialized knowledge and skills – with new ones always emerging. In a survey by the Ponemon Institute, respondents indicated that not having enough skilled professional dedicated to cybersecurity was the second biggest barrier to cyber resilience. Only 29 percent of companies reported having ideal staffing levels.¹

Consequently, a hybrid inside/outside model of cybersecurity defense and response is rapidly emerging. The hybrid security model fluidly brings together the right combination of internal staff and outsourced experts to handle a given situation, whether for long-term preventive planning, in-the-moment incident response or anything in between.

This paper explores why the older “all or nothing” kind of relationship between business organizations and information security services providers (ISSPs) is giving way to a hybrid model that security professionals can leverage to augment their operations and effectiveness.
Lack of investment in new cybersecurity technologies and inability to hire and retain skilled professionals are the biggest barriers to cyber resilience.

### What are the biggest barriers to cyber resilience?

Three choices allowed

<table>
<thead>
<tr>
<th>Barrier</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of investment in new cybersecurity technologies, including AI and ML</td>
<td>60%</td>
</tr>
<tr>
<td>Inability to hire and retain skilled personnel</td>
<td>56%</td>
</tr>
<tr>
<td>Lack of visibility into applications and data assets</td>
<td>46%</td>
</tr>
<tr>
<td>Lack of training for end-users</td>
<td>31%</td>
</tr>
<tr>
<td>Lack of training and certification for IT security staff</td>
<td>28%</td>
</tr>
<tr>
<td>Silo and turf issues</td>
<td>24%</td>
</tr>
<tr>
<td>Lack of information governance practices</td>
<td>22%</td>
</tr>
<tr>
<td>Lack of board-level reporting on the organization's state of cyber resilience</td>
<td>17%</td>
</tr>
<tr>
<td>Lack of C-level buy-in and support for the cybersecurity function</td>
<td>15%</td>
</tr>
</tbody>
</table>

In Cybersecurity, DIY Is DOA

As cyber threats multiply and the consequences of a breach rise – reputational damage, loss of intellectual property (IP), noncompliance ramifications, class action lawsuits – most organizations are discovering that do-it-yourself (DIY) information security simply isn’t an option.

Even for those few organizations that can justify the investment, DIY cybersecurity is off the table due to the scarcity of needed talent. The problem: increasing cyber threats and borderless enterprise networks have dramatically increased the complexity of the information security challenge – and the specialization of knowledge needed to meet it.

“There just aren’t enough security experts to hire on the entire planet for every large business to do their own custom threat intelligence,” says Alex Tilley, E-Crime Lead for Secureworks™, an information security services provider (ISSP). ISSPs offer threat intelligence as a service that businesses large and small use to inform and empower their internal resources.
**Threat Intelligence:** Gathering, interpreting and applying intelligence about cyber threat activity going on around the world in order to continuously refocus your cyber protection investment and resources as the threat environment evolves.

**Monitoring and Alerts:** Implementing, configuring and maintaining security monitoring appliances and then analyzing their output to identify threats inside your organizational network, and prioritize them all according to the enterprise risk they represent.

**Incident Response:** Responding rapidly to high-priority threats to mitigate potential consequences – especially to brand reputation.

Each of these broad buckets breaks down into multiple sub-specialties that demand specific knowledge and skills of their own. Further exacerbating the challenge is a proliferation of platforms, devices and environments. Jeff Carpenter, Senior Director for Threat Intelligence and Incident Response for Secureworks, explains: “Any large business will need Windows, Macintosh and Linux skills – but a Windows expert may not have the skills to analyze a Mac environment. And in mobile, iOS, Android all add additional complexity and knowledge requirements.”

**Hybrid Security Models Gain Acceptance**

Given the deep knowledge and technical skills required across such a diverse range of specialties, more and more businesses are choosing to partner with ISSPs in hybrid inside/outsourced cybersecurity models.

To do so, however, organizations typically must overcome internal issues such as budget considerations, or a hesitancy to give up head count on the part of whoever leads the organization’s security. And then there’s the biggest obstacle of all: “Until they actually try it themselves and run into a serious threat, most organizations simply can’t quite grasp how hard it is to do comprehensive cybersecurity really well – or to find the people with the skills to do it,” notes Terry McGraw, Vice President, Global Cyber Threat Research and Analysis at Secureworks.
But organizations are rapidly overcoming such obstacles, because hybrid models allow them to invest in the resources that make the most strategic sense and mitigate areas of greatest risk for their particular industry, operations and culture. Further, ISSPs offer a ready source for those aspects of cybersecurity that are simply better when done by outsiders, such as incident response planning and testing.

“It’s hard to test if you’re using your own people to develop the exercise and participate in the scenario,” says Carpenter. “They’re the people you want to test.”

Onboarding with a New ISSP

Getting the most out of a new ISSP agreement requires overcoming the same kinds of issues that plague any new relationship. As Secureworks’ Terry McGraw explains it, most new clients are unprepared for the volume of alerts they receive in the first few days unless there’s been excellent communication and mutual understanding built up in the onboarding process. That enables pre-tuning systems and processes with insights about your unique risk profile and specific concerns. Also important is a focus on change management for your internal processes, procedures and personnel, so that your organization can better exploit the value offered by the ISSP. “There usually is a good period of time before we reach steady state with a new client,” says McGraw.

“Until they actually try it themselves and run into a serious threat, most organizations simply can’t quite grasp how hard it is to do comprehensive cybersecurity really well – or to find the people with the skills to do it,”

Terry McGraw
Vice President, Global Cyber Threat Research and Analysis, Secureworks

Services Designed for Collaborative Integration

Given the diverse specialties and team-oriented nature of Grade-A cybersecurity, ISSPs such as Secureworks have designed their services from the ground up for collaboration with clients, and to flexibly adapt to support every client’s unique security needs.

A client’s internal staff, for example, is the primary user of threat intelligence services, which essentially extends the eyes and ears of your internal security team outside your organization. And Secureworks incident response teams decide what services to deliver in a collaborative scoping meeting that kicks off their joint response activity. “That’s the point where we develop the detailed response plan for that particular incident, determine the client’s gaps and what we should bring – all of which might change over time and based on the details of an incident,” he says.

The following overview of selected services from each of the three broad buckets clarifies how broadly, or narrowly, businesses can tap into outside cybersecurity expertise.
Threat Intelligence Services

These are typically based on the Secureworks Global Threat Intelligence information feed (the same for all clients) containing up-to-the-minute assessment of cyber activity around the world. As Tilley puts it, “Our Global Threat Intelligence feed puts threats on clients’ radar as they emerge. From everything that might be attacked, it tells clients what things threat actors are actually choosing to attack, and includes detailed threat indicators that clients can use to hunt for those threats in their environments.”

The global feed also includes software vulnerability information that clients can input into their patch-management processes.

• Clients can go beyond the global feed to customize the threat intelligence flowing from their “extended eyes and ears.” Some examples include:
  • Enrichment support services that answer clients’ specific questions
  • Attacker data feeds that can insert emerging threat indicators directly into client security controls
  • Borderless threat monitoring to alert for any global cyber threat activity related to client-defined keywords
  • Enterprise brand surveillance, which monitors open sources (such as social media) for cyber activity related to the client’s brand

Monitoring and Alerting Services

These break down into two major buckets of their own, each of which can be delivered at any point on a spectrum from 100 percent outsourced to just a tiny sliver. McGraw points out that, “We embed our staff [residency] with some clients to provide in-depth service, and with others we just fill in on nights and weekends, or when an internal person goes on vacation or is out sick.” The two buckets are:

• “Eyes on Glass”: Monitoring and interpreting firewall and Intrusion Detection System (IDS) data and differentiating between relatively benign or malignant threats, and deciding when to alert
• Remediation: Fixing the problem on all devices covered by a managed services agreement, and alerting internal staff to fix servers and endpoints not covered

The immediate value an ISSP brings to monitoring and alerting services comes mostly from their hard-to-find experts “who can stare at network package capture data and actually understand the malicious behavior that is presenting itself,” says McGraw. “There are only a few thousand SANS GCIs in the world – and that certification is merely the baseline for our analyst hiring process.” GCIA is a nested acronym: it stands for GIAC Certified Intrusion Analyst, and GIAC stands for the Global Information Assurance Certification (which grew out of the work of the SANS Institute).
The stark difference that ISSP expertise can bring to a business may be best seen in the following statistic. McGraw says that when a new client brings in his team and they detect a threat, “The average time an advanced persistent threat has been on their network is approximately 191 days. So threat actors were in their environment already and they didn’t know it.”

**Incident Response Services**

These services demonstrate the fluidity of ISSP-client hybridization at an extreme. As already mentioned, at the outset of any incident response a scoping meeting takes place that determines precisely what services the ISSP should provide, given the client’s resources and the exact nature of the situation. The incident response roles and expertise a client might tap from an ISSP include:

- **Forensic Analysis of Systems and Networks:** Determining how intruders gained access and what they did (including whether data was compromised)

- **Intelligence Analysis:** Identifying specific adversaries and recommending remediation based on deep knowledge of many adversaries’ tactics and techniques

- **Malicious Code Reverse Engineer:** Dissecting malicious code to fully understand what it is doing and how to thwart it

- **Incident Commander:** The incident response team leader, capable of making sound decisions based on experience and expertise in handling intense, high-pressure situations – think Gene Kranz, the flight director for Apollo 13

- **Planner and Tester:** Develops the response plans that encompass all appropriate departments of your organization – including HR, legal and external communications – and oversees periodic drills to assess response performance before you’re in a real firefight (see callout above: Testing Like A Firefighter)

“**For most of our clients, we’re performing roles that require special skills that they can’t or don’t want to hire,**”

Jeff Carpenter
Senior Director for Threat Intelligence and Incident Response, Secureworks

**Testing Like a Firefighter**

When Secureworks’ Jeff Carpenter isn’t fighting his clients’ cyber fires, he fights the hot kind of fires as a volunteer with Berkeley Hills Fire Company, just north of Pittsburgh – as he’s done for 29 years. That’s where he absorbed the philosophy of training and drilling that he always tries to instill in his clients. “You have to find out you have a capability gap in a drill – not when you arrive at the scene of a house on fire and it’s burning down,” says Carpenter, adding: “In the fire service, we practice every week. We do outside training where we go away to fire school. You have to do that because you simply can’t know that you can do the job until you test yourself.” Carpenter insists it’s the same thing with incident response. Organizations must develop enterprise-wide response plans, and then drill them regularly to identify underperformance and train up any weak links.
ISSPs perform the roles, requiring special skills, that most clients can’t or don’t want to hire. For example, a client may have an incident response person, but if that person doesn’t have malicious code reverse engineering skills, the next cyber incident may not be resolved as quickly as it would with a responder who has the appropriate skills.

**Conclusion: Collaborate to Win the War**

Wars aren’t won through individual heroics. It takes allies, teamwork and coordinated strategies and tactics to defeat determined, well-resourced enemies. In cyber warfare, there is way too much information to track and too many sub-specialties requiring in-depth skills and knowledge – all of which is continuously evolving in real-time – for any one organization to be able to win alone.

Therefore, leading organizations have become proactive about cyber defense and response by combining their internal resources with external expertise. They choose to partner with ISSPs that provide a full spectrum of cybersecurity services, but can fluidly carve out narrow slices so they get just what they need, when they need it, in ways that mesh well with their internal resources.

**Sources:**

1. Ponemon Institute, The Third Annual Study on the Cyber Resilient Organization, March 2018
Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer™.

<table>
<thead>
<tr>
<th>Corporate Headquarters</th>
<th>Europe &amp; Middle East</th>
<th>Asia Pacific</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>United States</strong></td>
<td><strong>France</strong></td>
<td><strong>Australia</strong></td>
</tr>
<tr>
<td>1 Concourse Pkwy NE #500 Atlanta, GA 30328</td>
<td>8 avenue du Stade de France 93218 Saint Denis Cedex +33 1 80 60 20 00 <a href="http://www.secureworks.fr">www.secureworks.fr</a></td>
<td>Building 3, 14 Aquatic Drive Frenchs Forest, Sydney NSW Australia 2086 1800 737 817 <a href="http://www.secureworks.com.au">www.secureworks.com.au</a></td>
</tr>
<tr>
<td>+1 877 838 7947</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>United Kingdom</strong></td>
<td><strong>Germany</strong></td>
<td><strong>Japan</strong></td>
</tr>
<tr>
<td>1 Concourse Pkwy NE #500 Atlanta, GA 30328</td>
<td>Main Airport Center, Unterschweinsteige 10 60549 Frankfurt am Main Germany 069/9792-0</td>
<td>Solid Square East Tower 20F 580 Horikawa-cho, Saiwai-ku Kawasaki, 212-8589 Japan 81-(44)556-4300</td>
</tr>
<tr>
<td>+1 877 838 7947</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.secureworks.com">www.secureworks.com</a></td>
<td><a href="http://www.dellsecureworks.de">www.dellsecureworks.de</a></td>
<td><a href="http://www.secureworks.jp">www.secureworks.jp</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>