CUSTOMERONE

Symantec

# Physical and Digital Security: We Just Call It Security

In 2015, an employee at our Symantec office outside Washington, D.C., wandered into an area where we store confidential information. He stopped at a restricted door and swiped his badge on the electronic card reader.

The door didn't open, but his effort did set off twin reactions: Our security team sent a guard to intercept him, and our cybersecurity team launched a quick digital investigation. The cyber team scoured his personnel file and, because he wasn't a U.S. citizen, looked for red flags such as connections to a foreign government.

As it turns out, there was no ill intent (he was just looking for the mailroom). But the incident demonstrates a key aspect of our security philosophy: When it comes to keeping Symantec safe we bring all of our intelligence resources to bear.

Our physical- and cybersecurity teams used to be separate, but in 2015 we brought them together as close partners. It's not a common business model—but we think it should be. In this day and age, if your security teams are operating in discrete silos you're not using your resources to their fullest. After all, it won't do you much good to have the strongest cybersecurity on your networks, if you also have employees who hold secure doors open for strangers.

In this paper we'll explain our security strategy and how it can work for you. We're limited on how much detail we can reveal here, but for more information you can schedule an executive briefing where we can answer your questions in depth. We can also come to your site and give you a personalized audit of your security setup.

---

Symantec is well-known as a cybersecurity company, but our goal is to be a *complete* security company, one that protects against physical as well as digital threats. We've spent the last year developing and fine-tuning a comprehensive strategy for ourselves that does just that. Now we're ready to share our best practices with you.

## If Your Security Posture Looks Like This, There's Room to Improve

When your company has a security issue, who do you call?

The answer we usually hear from customers is: "It depends—if it's a cybersecurity issue we call IT, and for an actual threat on campus we call physical security."

Here's the flaw: By treating the two security teams as separate entities you're overlooking the fact that many threats have both physical and digital implications. For example, someone who's trying to badge into a restricted server room might be trying to commit espionage by downloading corporate secrets onto a thumb drive.

So the better answer is to create a single security office to which employees report every issue. Then staff that office with people from both your cybersecurity and physical-security teams.

That's how we do it. As a matter of fact, within Symantec we rarely draw a distinction between physical security and cybersecurity.

We just call it security.

## Securing Your Company by Tracking Employee Behavior

Like you, we need to protect ourselves from a full range of onsite threats: a rogue employee looking to download confidential information and defect to a competitor, an outsider sneaking in and stealing intellectual property, or an Edward Snowden-style attack.

Let's consider the Snowden case. Politics aside, the facts are these. He stole digital information, a failing of the NSA's cybersecurity team. But there were other behaviors as well, which the physical-security team should have investigated. He started coming into the office at odd hours; he requested 24-hour access even though he had no business need for it; and he tried exploring areas of the building where he didn't have proper clearance.

The NSA's physical-security team did notice his odd behavior but didn't alert the digital-security side, for two reasons. One, it assumed the threat was confined to the physical side; and two, there was no policy spelling out how and when the two teams should collaborate.

Had the teams combined forces in time they might have averted the espionage. Instead it became front-page news all over the world.

Security usually boils down to human behavior. Rogue employees who want to steal digital information often leave clues in their day-to-day actions. They may start coming in when no one else is around, or they may try to access secure areas. These are red flags that demand further investigation. *(See Sidebar: What You Don't Know Can Hurt You.)*

That's why it's so important for your physical- and cybersecurity teams to collaborate. To do it right you'll need policies that define:

- what information they exchange, and how often
- how each team will respond to various security alerts
- when one team ought to involve the other in an investigation

## Monitoring for Pre-Targeting Indicators

At Symantec we used to have separate security teams. They operated in disconnected silos and each had its own Security Operations Center, or SOC.

Our first step toward collaboration was to combine the two SOCs in early 2016. Next we instructed our cyber team to

## What You Don't Know *Can* Hurt You

When Symantec's head of physical security visits customers they're often eager to show him their security setups. But it rarely takes him long to find a gap—even at some of the nation's top tech companies and government contractors.

If anyone knows security risks, it's John Eversole. An Army reservist and former Marine, John ran security for the chairman of the U.S. Joint Chiefs of Staff; he was the personal bodyguard for a U.S. secretary of defense; and in the corporate sector he directed personal security for one of the richest CEOs on the planet.

He came to Symantec in 2015 to help us develop security solutions for the rest of the business world.

When he talks to customers he starts by asking whether they can list every person who has access to the company's sensitive spaces. They usually say yes.

"Well," he asks, "do you know the person who picks up your trash? Does that person have a master key? Do you let them go anywhere, including your executive offices, without keeping tabs on them? Do you know what they're doing with your garbage?"

The executives usually fall silent.

John notes that janitors are generally low-paid. So a criminal looking to commit espionage could tell them, "Here's $20,000—get me pictures of the inside of the CEO's office. Then

*continued on page 6*

create automated dashboards, which track internal data and convert them into information our physical-security team can use to make investigative decisions.

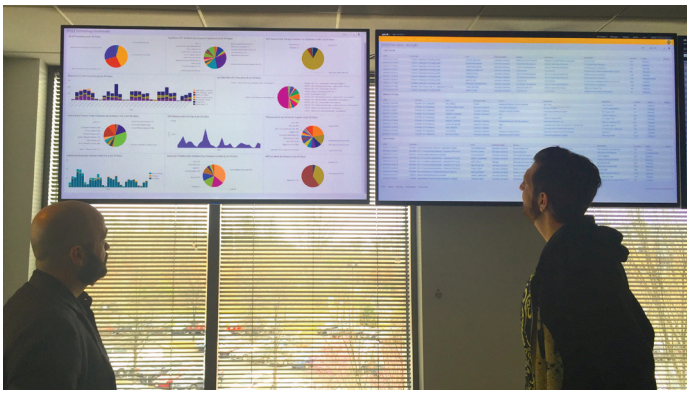
Some dashboards are specific to employee activity, for example:

- which employees, by site, ask for 24x7 access
- whose access attempts during regular hours are denied most often
- which employees are denied after-hours access

Others track access points such as:

- which doors get propped open most often
- whether any door loses communication with our security network
- which sites—and which specific doors—have the highest rate of badge denials
- whether a deactivated badge gets used in an access attempt

You can tell from our dashboards how aggressive we are about investigating failed badge-in attempts. Customers are sometimes surprised to learn that. After all, they say, if a badge can't open a restricted door, does the failed attempt really matter?



***Physical security teams up with cybersecurity:*** *At our Security Operations Center in Virginia, John Eversole, our head of physical security, and SOC manager Jacob Horst, study dashboards that track security conditions at Symantec sites around the world.*

"Absolutely," says John Eversole, our senior director of physical security and safety. "Badging attempts can be a pre-targeting indicator—a test of security policies to determine how to defeat them. A true bad actor might test a restricted door multiple times, maybe to see if the security system is ever turned off or is acting erratically."

So we implemented a three-step process called **threat modeling**. It involves identifying the areas where a breach could be most damaging; developing policies to safeguard those areas; and reinforcing employee behavior to ensure the policies are always followed.

## Using Teamwork to Keep Symantec Safe

Here are two simple examples of how we use our merged security team to enhance our intelligence and keep Symantec safe.

During a review of our worldwide offices in early 2016 our cyber team noticed that one of our Chinese offices was giving out badges with generic names such as Tea Person rather than using the vendor's real name.

It seems like a minor issue but it elicited a major response from our security team. Rightfully so, says Jacob Horst, who runs our Security Operations Center in Virginia.

"Badges are important—they're the keys to the building," Jacob says. "We can't have any ambiguity at all. Someone on site may know who these people are but if we don't know here at the SOC we need to make sure our local security people go in and enforce the policy of only using real names."

So that's what we did. Our physical-security team identified every temp who was using a generic badge and then provided each person a personalized badge and unique employee ID number.

Here's another example. In late 2015, engineers at our site in Springfield, Oregon, were using equipment that detects wifi hotspots. It was part of a red-team effort to identify vulnerabilities, both digital and physical, across our campuses.

They happened to come across a mysterious hotspot that was accessible from the parking lot. A quick test revealed it wasn't an approved Symantec hotspot, and it shouldn't have been active in that area.

They reported their findings to our Security Operations Center. The SOC team was able to track down the offending wifi device that, it turns out, had been deployed by a previous employee but not disconnected when the employee left the company.

This is how our teamwork with physical security makes us stronger. Our security guards already crisscross our campuses as part of their regular rounds, so we now equip them with the same detection technology the red-team engineers were using. Now our security guards are playing a key role in monitoring our digital security.

## Security Guards—An Untapped Resource

We've noticed that a lot of companies underuse their security guards. At Symantec they're an integral part of our security. In fact, even though they're mostly contractors, we empower them to enforce some of our most important policies.

For example, we ask them to watch for tailgating (in which a person follows someone else into a building without badging in himself or herself). The guard's job is to remind both parties that tailgating is a strict policy violation, and to report repeat offenders. Even when employees badge in appropriately our guards randomly check their IDs to make sure they're not using someone else's badge.

We also ask our guards to remind employees not to walk away from their computers and phones. At our California headquarters, guards will hang a tag on unattended computers to remind employees to be more careful.

The guards at our Oregon site go a step further. Employees there will often work in a conference room, and occasionally they step away


and leave their laptops unattended. If that happens, a guard will lock the door and leave a note instructing them to contact security to open it.

Employees hate the inconvenience—but they rarely make the same mistake twice.

## Executive-Safety Checklist

In September 2015, an al-Qaeda group called for the assassination of U.S. executives as a means to destabilize the American economy.

Six months later, a group of ISIS supporters issued veiled threats against the CEOs of Facebook and Twitter. The group posted images showing the CEOs' photos engulfed in flames or riddled with bullets.

Threats like these are growing. They reinforce the need for every company to review its executive safeguards and develop the strongest precautions possible.

Here are a few practices we ask our Symantec executives to follow, especially when they travel abroad:

**At home:**

- Vary your route to and from work; have at least four different routes
- Leave random lights on at night to avoid predictability inside
- Avoid going to the same location for services (haircut, grocery, gym). If you must use the same location, vary your arrival times by at least an hour

**Pre-travel:**

- Have your office ensure that the driver at your destination speaks your native language and understands your itinerary from start to finish
- Use only "clean" (company-owned and -protected) devices to access email and data so your network can't be compromised by foreign intelligence

**At the airport:**

- Always keep a close eye on your belongings. Be careful if someone approaches you with a question, as his or her intent could be to distract you
- When taking a taxi always keep your luggage in the trunk, especially your laptop. If you use your mobile phone keep it away from the window

**In public areas:**

- Try not to discuss company business, especially if it involves money or intellectual property, near people you don't know
- Avoid talking to strangers, especially those who are insistent

**Other precautions:**

- Avoid demonstrations and protests, especially if they appear political in nature
- Know the location of your nearest embassy or consulate as a rally point for emergencies

As much as we rely on our guards, however, we don't place the entire security burden on them. Ultimately it's up to employees to follow our policies.

"My security force's job is to remind you, the employee, that you're a security practitioner too," says Robert Odwyer, who runs our global physical-security operations. "That's our whole philosophy."

## A Strong Security Policy Improves Employee Loyalty

There are obvious benefits to strong corporate security. There are less obvious benefits too, as we learned when we extended our security policy to our international offices.

Security at our non-U.S. sites used to be run by a patchwork of vendors. Their services were inconsistent from one site to the next, and it was hard to hold them accountable from our California headquarters.

Part of the reason we hired Robert was to streamline our global process. He found a single security provider that offers consistent, culturally sensitive services around the world. By consolidating our vendor contracts we saved hundreds of thousands of dollars, and we also have the comfort of knowing our security services are consistent from one global office to the next.

It's hard to overstate the importance of a global view of security. From the attacks in San Bernardino, California, to fires in Dubai, to terror threats at Munich train stations, we've worked hard to keep local employees safe. We help them with evacuation plans, emergency lodging, and anything else they need.

For example, during the Paris terrorist attacks in 2015 we called every local Symantec employee, some of whom confessed their fears and asked that we stay on the line until they got assistance. And when floods in India left about 70 employees trapped in our Chennai offices for three days, we made sure they had food and water and that their families were safe.

"Our first priority and driving motivation is to ensure the safety of our employees, I want to be clear about that," says Tim Fitzgerald, our chief security officer. "But beyond that, think of the loyalty we create when we're able to help someone on a personal level. People gain an incredible level of trust in our organization, and the relationship that gets forged helps us create security evangelists for both physical and cybersecurity."

## Next Steps: How You Can Incorporate Symantec's Security Strategy

There's a lot to think about when it comes to strengthening your own security. But since we've gone through it ourselves, we can help you learn from our experience.

The first thing you'll need is an audit of your current security setup. We can come to your offices and provide customized recommendations and advice. Or you can visit us and we'll walk you through our setup in more detail than we can reveal in this paper. We'll tell you what worked and where we saw room for improvement, and we'll teach you our best practices so you can get up and running even faster than we did.

We have Executive Briefing Centers at our U.S. headquarters in Mountain View, California, and in Reading. We'll be happy to tailor your experience to your company's specific needs.

Contact Symantec today.

customer_one@symantec.com

CustomerONE Team
350 Ellis Street
Mountain View, CA 94043
800-745-6054

Symantec's CustomerONE team can facilitate discussions between you and our IT security practitioners to help you address your security questions and concerns. Please contact us directly or through your Symantec sales team.

Copyright © 2016 Symantec Corp. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corp. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

## What You Don't Know *Can* Hurt You *continued from page 2*

tomorrow, for another $20,000, let me into the office for 20 minutes so I can plant a listening device or collect intelligence." How many janitors would say no?

If this sounds more Hollywood than real-world to you, think back to the headlines from last decade. That's when Oracle CEO Larry Ellison called a news conference to boast that his team of investigators had just acquired incriminating documents against Microsoft—and they did it legally. All they did was visit a Microsoft partner and pay a janitor $1,200 for a peek at the trash.[1]

### Maintaining Healthy Paranoia

Let's consider a pair of less theatrical dangers: internal espionage and security gaps.

First, rogue employees could be looking to steal intellectual property or sell your confidential information. Either way your solution is simple: Know where your most critical physical data resides, and then restrict access to those areas so tightly that even the janitor can't get in without a security escort.

Second, even the most thorough security plan has gaps. The best way to tease them out is to cultivate a sense of vigilance, almost to the point of mild paranoia, in your security team.

Here's a quick example. At our headquarters, an employee who forgets his or her badge is given a temporary badge with appropriate access permissions (that expire at midnight). At the end of the day the employee returns the badge to a locked box in the lobby.

Robert Odwyer, our head of physical-security operations worldwide, happened to notice that the drop-off box in his lobby wasn't affixed to anything. He picked it up, shook it upside-down, and three or four badges fell out.

That was a valuable lesson. Now we bolt the boxes down so they can't be shaken.

"If I want to break into your space, those are the sorts of things I'd look for," Robert says. "I'd test what worked and didn't work, who's being vigilant, who's not. You always have to be doing these what-if scenarios."


*A receptionist poses next to an old badge box, which hadn't been bolted down, and its secure replacement.*

### Security Cameras Can Fall Short

One last note: Security cameras are a popular option, but understand their limitations.

Cameras are meant to do two things: serve as a deterrent and provide forensic evidence after a crime. The level of deterrence is questionable—after all, stores like Wal-Mart have scores of cameras but they still report millions of dollars of shoplifting losses every year. And while post-crime evidence is helpful, your goal should be to prevent crimes in the first place.

In other words, don't think you're fully covered just because you have cameras installed.

[1] "In AP Interview, Oracle CEO Larry Ellison defends Microsoft probe," by Michael Liedtke, June 29, 2000: http://bit.ly/21DLHy4