Chapter 1

WELCOME TO THE PERFECT STORM

IF YOU WORK IN IT, YOU’RE PROBABLY FAMILIAR WITH THE NUMBERS.

Online attacks claim 1.5 million victims every day and add up to $110 billion in losses every year. Cyber attacks grew 23 percent last year—and 138 percent on mobile devices. And 2013 has (unfortunately) become known as the year of the mega-breach, with 253 breaches that exposed more than 10 million identities. These facts and figures all point to one inevitable conclusion: cyber criminals are more intelligent, organized, and aggressive than ever before—and in far too many cases they’re winning.

But that’s only part of the story.

In the face of these growing threats, we’re in the middle of a full-blown mobile revolution. One-third of the world’s five billion mobile devices are Internet-connected smart phones, and millions of workers use those devices to collaborate and access sensitive data and systems every day. That’s no surprise. There is a huge, obvious competitive upside to an always-connected, totally mobile workforce. But mobile agility and productivity are mirrored by all kinds of new vulnerabilities and risks. And unlike the past, your ability to control these devices and the people who use them is limited—or non-existent.

So essentially, you’re caught between Internet-addicted users who are demanding even more flexibility and freedom—and smart, organized criminals who are fully prepared to pounce on all the new risks and vulnerabilities they create.

It’s a perfect storm. Our industry has never experienced anything quite like it. So now the question is, what are you going to do about it?

CYBER CRIMINALS ARE MORE...

INTELLIGENT In 2013 there were 253 breaches that exposed more than 10 million identities.

ORGANIZED Cyber attacks grew 23 percent last year—and 138 percent on mobile devices.

AGGRESSIVE Online attacks claim 1.5 million victims every day and add up to $110 billion in losses every year.
What does your cyber security future look like? The answer is not bigger, better point security products. It’s not heavy-handed mandates or stricter IT controls. And it’s certainly not larger IT budgets or head counts. These traditional security tactics and methods are failing. Their weaknesses are becoming more glaring and dangerous as criminals grow bolder and people become more mobile and connected. And your business deserves better.

Minimizing the risks of future cyber attacks requires a fundamental change in the way you think about security—from a defensive posture that attempts to block all malware to a more realistic approach that focuses on making your organization cyber resilient.

What does that mean? It obviously means doing everything in your power to block malicious attacks. But a cyber resilient approach also recognizes that in today’s world, no amount of time, effort, or money can guarantee success—and that breaches have basically become inevitable. So in a cyber resilient environment, you go beyond prevention to minimize the chances of a breach succeeding. And even if it does, you make sure you can react and recover quickly with minimal damage.

Cyber resilience focuses on managing risk, which is realistic—rather than totally eliminating it, which is not. It offers you more freedom to empower your connected, mobile users and offer them the services and access they need. And it gives you new flexibility to find the right balance between agility and risk based on the unique nature and needs of your business.

Chapter 3
INTELLIGENCE DRIVES RESILIENCE

Security intelligence is the engine that powers cyber resilience. With better intelligence, you can make smarter decisions, improve your organizational processes, and dramatically increase your ability to block and respond to attacks.

Of course, security intelligence means different things to different people. For some, the definition is limited to data about local and global security vulnerabilities and threats. But true security intelligence goes beyond data—to fully encompass people, processes, and technology.

In this expanded view, all of the people in your organization understand and support security best practices—which translates directly into more intelligent decisions and lower risks. Effective security processes build and strengthen your cyber resilience. And all of your security technology works together to protect, detect, and respond quickly to threats.

This broad approach to security intelligence combines and unifies all of the best people, processes, and technology from inside and outside your organization to help you achieve true cyber resilience.
YOUR INTELLIGENT PATH TO CYBER RESILIENCE

Cyber resilience isn’t a visionary pipe dream, but it’s not a static checklist either. Instead, it’s a practical, achievable framework—based on five best practice-based pillars—that you can start building and strengthening today. Even better, it’s designed to facilitate continual, ongoing improvements that adapt to the changing cyber landscape.

**PREPARE:** Accurately assess your security vulnerabilities, educate your employees, and review your processes.
Before you can move toward a cyber resilient organization, you have to accurately assess your current situation. This process starts with a thorough infrastructure and information assessment that identifies and highlights all of your security vulnerabilities, but it should also include efforts to evaluate your employees’ security IQ and measure the effectiveness of your critical processes (like backup and recovery). With this information, you can establish a baseline, compare the results with your peers, and begin addressing the most urgent issues.

**PROTECT:** Upgrade and unify your security systems and solutions.
After you assess your biggest security weaknesses and priorities, you can start developing and implementing safeguards for your most critical infrastructure components and services. Depending on your situation, this could include upgrades to your existing prevention solutions, efforts to unify disjointed point security products, or initiatives to automate security policy enforcement.

**DETECT:** Leverage data-level integrations and security intelligence to identify attacks and breaches.
Intelligent detection goes beyond the traditional threat-blocking paradigm—by leveraging embedded detection capabilities, data-level integrations, and correlated security intelligence to rapidly identify attacks and breaches, find out which systems have been affected, and mount a fast, effective response. This stage also focuses on measuring and assessing the safeguards you have in place, so you can make continual improvements to your threat protection and security intelligence processes and technology.

**RESPOND:** Combine planning, people, and automated processes to remediate incidents quickly.
Effective cyber detection is only as valuable as your ability to mount a timely response. Cyber resilient organizations combine effective cyber incident plans, knowledgeable and well-trained people, and automated processes to remediate incidents quickly and with minimal damage. They understand the value of working with a proven outside incident response service that can provide extra on-demand assistance when needed. And they know how to incorporate the lessons they learn from attacks into future responses.

**RECOVER:** Restore lost data and damaged systems with minimal impact to your business.
No matter how well you plan and prepare, you can never guarantee your immunity from cyber attacks and their damaging effects. The recover stage works to make sure you can restore lost data and damaged systems quickly—and with minimal impact on your business operations, reputation, and bottom line. Cyber resilient organizations already know which systems and data are most critical to their business operations (from the preparation stage), and they’re prepared to restore those resources first.

**Effective security processes build and strengthen your cyber resilience.**
Chapter 5

A CYBER RESILIENCE PARTNER YOU CAN TRUST

Cyber resilience is not about finding some magical combination of point products or technologies. It’s about understanding and recognizing today’s cyber security realities—and then bringing people, processes, and technology together in ways that maximize your business agility and minimize your risks.

Symantec is uniquely qualified to help you do that—with more than 25 years of cyber security experience, the world’s largest source of global security intelligence, and a broad, proven technology portfolio that goes far beyond traditional malware protection.

So find out what we can offer your organization. And begin your journey toward a cyber resilient enterprise today.

Symantec is ready to offer you:

**Proven solutions**—with an unsurpassed breadth of market leading security products and services to meet any security need and address all five stages of the cyber resilience framework.

**Leading Competencies**—with expertise and capabilities no other security vendor can match. This includes:

- External threat data collected from millions of sensors around the world
- Big Data analytics powered by multiple Security Operation Centers (SOCs) around the world
- Military grade data centers that support leading cloud-based services
- Hundreds of security experts who are standing by to help you identify threats and assist you with remediation

**Impressive Scale**—with 20,000 employees, a presence in 50 countries, and the ability to track 3.7 trillion threat indicators annually. When you do the math, it’s clear that Symantec is in the best possible position to protect your information, wherever it’s stored or accessed.

IT’S A PERFECT STORM. OUR INDUSTRY HAS NEVER EXPERIENCED ANYTHING QUITE LIKE IT. SO NOW THE QUESTION IS, WHAT ARE YOU GOING TO DO ABOUT IT?