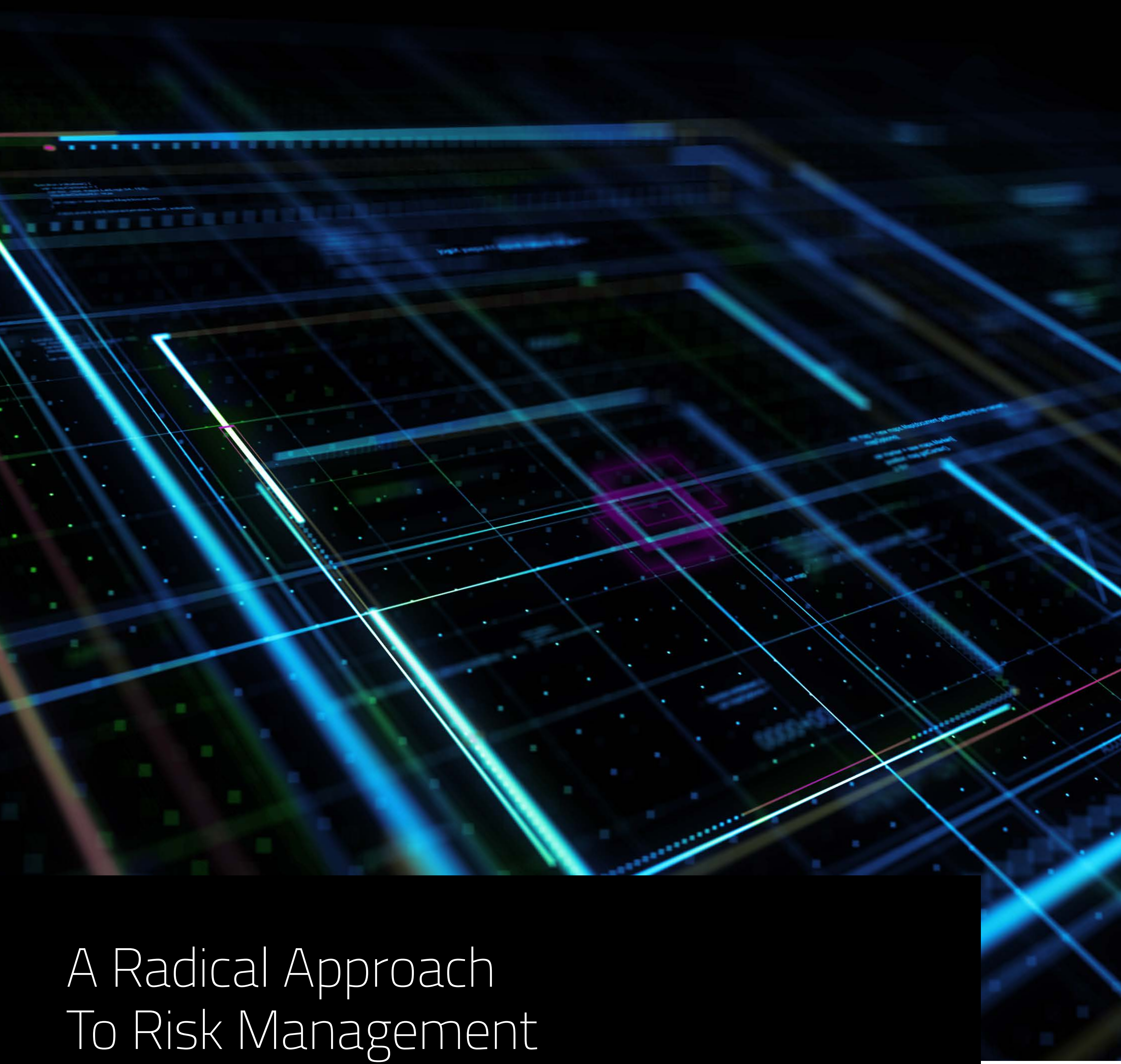


# A Radical Approach To Risk Management

## How Traditional Controls Fail and Why Security Will Never Be the Same

CYLANCE™

## Introduction

The world of cybersecurity has changed. Cybercriminals today target organizations and unleash a torrent of malicious files and attacks that flood an enterprise until a breach occurs. They have learned to automate the production of malicious code and vary it just enough to create never-before-seen or unknown attacks. Many businesses, whether small, mid-sized, or large, have been infiltrated without detection. Today's risk management leaders need agile defenses that quickly adapt to these new demands and stay ahead of attacks. Yet, threats are only part of the story. The ever-changing technology landscape adds complexity for the CISO, CIO, and IT leader.

The future of information risk requires radical change to face the modern landscape. It means gaining a level of understanding and a new model for assessing conditions and moving forward.

## The Rise of Risk

The issues of information risk and security are no longer concerns for only IT companies or government organizations. The world has gone digital. Manufacturing, retail, food services, and industries once thought beyond the providence of data services have turned a corner. For example, Oscar Meyer offers a dating app to help bacon lovers meat (pun intended) one another. 'The Scarecrow' microsite from Chipotle is an online game, a short film, and a project that reflects, per the website, "what we believe in".

Whether it's the Chief Information Officer at Oracle, OPM, or Chipotle and Oscar Meyer, executives face the business challenge of securing data, employees, and customers. Indeed, security professionals have become the front-line defense against cyberattacks. More companies today have expanded budgets, people, and processes to wage war against the myriad of threats that would do harm.

For many, the battle against breaches is not being won. Some of the high-profile security breaches that have caught the attention of national media include:

- The United States Office of Personnel Management (OPM)
  - In 2015, the U.S. government revealed that attackers had stolen files from the Office of Personnel Management for 21.5 million current and former federal employees
- JP Morgan Chase
  - The 2014 JP Morgan Chase data breach is believed to have compromised data for an estimated 83 million accounts
- Anthem, Inc.
  - Anthem disclosed in 2015 that attackers had broken into its servers and potentially stolen over 37.5 million records (Anthem later raised the number to 78.8 million records)
- eBay
  - In 2014, eBay requested 145 million users change their passwords as a 'precautionary measure', but it was not sure how many accounts were compromised
- Target
  - In 2013, attackers stole information on up to 110 million customers during the holiday shopping season

The successful breaches occur, in part, because bad actors today continuously adapt attacks and increase attack frequency. Attackers today develop threats that target a single enterprise. They automate the creation and sending of multi-variant malicious code that overwhelms traditional network security until a breach occurs. And the reality is many businesses, from mid-size organizations to multi-national brands, have likely been infiltrated without detection.

Leaders tasked to protect precious data and systems can't adjust defenses to keep up with the new threat demand.

With the rise of successful enterprise attacks, a new approach is needed; one where **protection enables the mission** across the entire organization, and security is viewed as a strategic process and function rather than a departmental goal, objective, or set of tactics.

## A Failure To Prevent Attacks

Many companies detect and respond to cyberattacks, but cannot prevent them. For decades, the antivirus industry was built on the concept of detection and response — and all technology, solutions, and services operated under this paradigm. In addition, previous attempts to prevent threats failed.

By employing traditional security, organizations expose themselves to high risks and long-term costs, since they react to attacks that infected at least one employee, known as the proverbial 'sacrificial lamb'. Detecting incidents after they have successfully breached the network both strengthens attacker's chances of success and weakens target companies against cyber vulnerabilities.

So how do you transcend a failed tactical approach when it's the singular paradigm in place within the global expanse of an entire industry?

The first step requires looking at how cybersecurity success is defined by examining security controls. Specifically, executives and IT staff should understand whether a control architecture improves or impedes business agility and velocity.

## The 9 Box of Controls Concept

A simple yet powerful framework, the 9 Box of Controls, looks at IT controls, including control types and automation approaches, the overall control architecture, and the significance of control friction on business productivity. It allows people to better assess the value and impact of information security controls on an organization. The concept was introduced with the publication of _Managing Risk and Information Security: Protect to Enable_ and has taken root among IT leaders across industries and geographies. As the concept gets shared with more businesses of every type, it drives security from a tactical conversation into a strategic, evergreen discourse about security spending, resource allocation, and long-term planning.

IT controls consists of any mechanism, policy, or procedure employed by an organization that affects the management processes for risk and security. IT or application controls seek to ensure that software used for processes, such as payroll, document sharing, or remote content access, are properly maintained, used, and protected.

The control architecture consists of types of controls and automation levels. The right control architecture enables improved threat management. As new attacks appear, IT can't stop the bad and allow the good without impacting users.

### Control Types

Security controls consist of three primary types:

- **Prevention** occurs when an action or control prevents an infection or cyberattack, stopping it before it affects people or the IT environment. Prevention centers on minimizing vulnerability from risk and the potential for harm.
- **Detection** identifies the presence of malicious code or files that have entered the environment. Detection focuses on minimizing damage after an incident has occurred.
- **Response** is the reaction to the discovery of malicious code. It attempts to remove it after a person or environment has been infected. With the reactive approach, the focus becomes detection and containment.

### Control Automation Levels

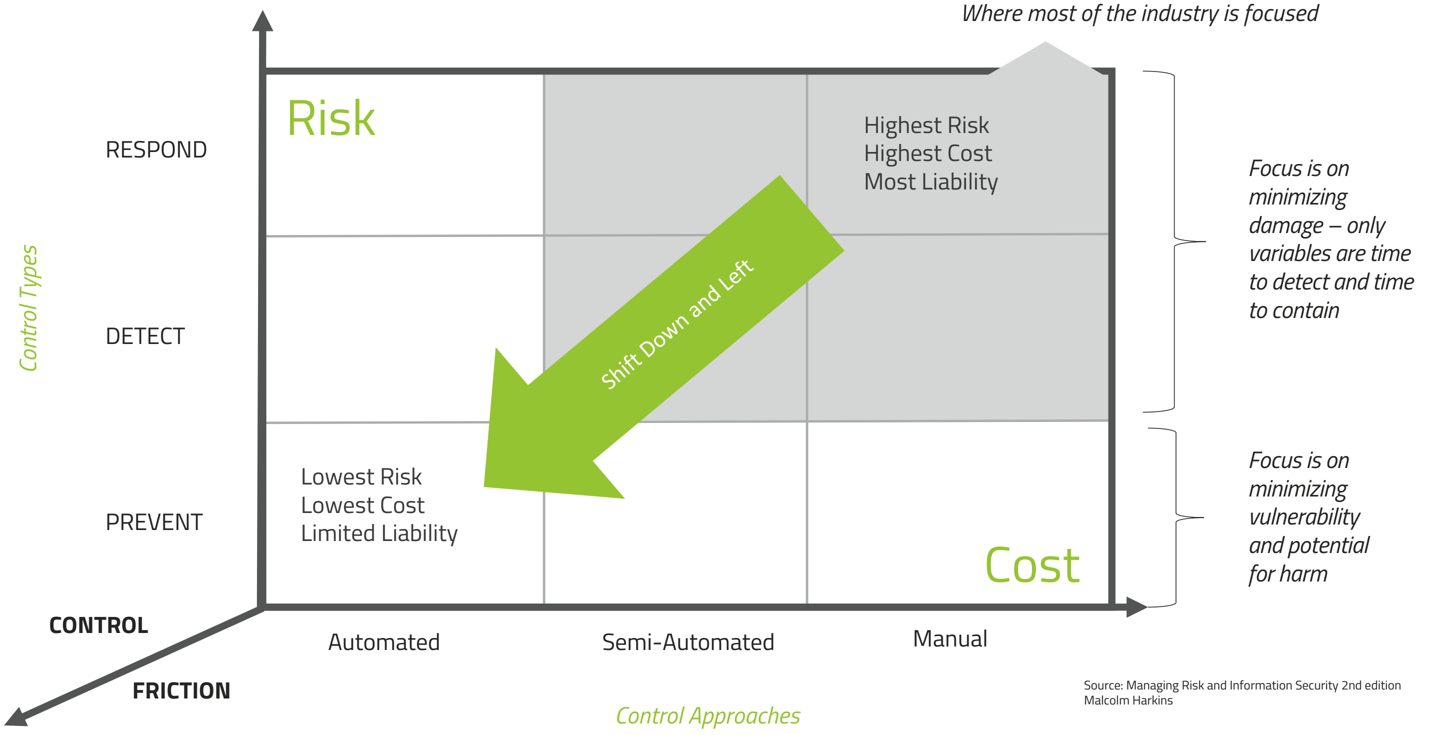
There are also three primary control approaches:

- **Automated** control occurs entirely through machines
- **Semi-automated** control involves a level of human intervention
- **Manual** controls are managed entirely by hand

The combinations of control types and automation levels comprise the cells of the 9 Box, as shown in the figure below. It represents how risk increases as an organization moves from prevention, to detection, to response. It also illustrates how cost increases as organizations move from automated, to semi-automated, to manual controls.

The development of IT controls and safeguards, as well as the different control automation levels, leads to another issue — control friction. When too many controls are put in place to provide security, the tipping point is reached, resulting in negative impacts. For instance, an organization puts into place the control policy of no information sharing by email. The control friction occurs when personnel from HR must save data to a protected server, set up by an organization's IT department, using a multi-step process that must be carried out for employees to access the data.

## 9 Box of Controls



Source: Managing Risk and Information Security 2nd edition
Malcolm Harkins

## The Key Dimension: Control Friction

Security controls can create control friction, or a 'drag coefficient', that impedes individual performance or business processes.

Think of the many examples of this. Device authentication and encryption controls aim to provide security yet require an inordinate amount of time and resources for IT departments, as well as bog down individuals trying to perform daily tasks.

Traditional AV tactics such as incremental storage, scanning machines, and re-imaging machines add to the drag coefficient. Large endpoint agents create performance friction for enterprise users because they occupy an enormous computational and/or data footprint.

When organizations apply too much control friction in the name of security, business users may choose to circumvent IT security controls. Here, the example of unintended consequences occurs. Company employees, and not IT, begin managing the technology they use, so data and business become isolated. When the security team loses visibility into the technology deployed by users, it cannot adequately prevent compromises, detection becomes more difficult, and response takes longer and requires more resources.

High-friction controls create the long-term effect of systemic business risk and it hinders business velocity. Organizations lose the ability to innovate, go to market in a timely fashion, respond to customer demands and industry forces, and lead the marketplace.

## Think Inside the Box

With the 9 Box of Controls paradigm, you can see how the traditional cybersecurity and antivirus industry profits from a detect and respond paradigm. Vendors have no real economic incentive to innovate, solve the core problem, or deliver prediction and prevention. If the number of attacks increases, you need more layers of technology, more solutions, and more tools in the toolkit to build greater protection. The model inherently keeps focus off the foundational issue with fixing the core vulnerability of insecure computing. A few solutions have entered the market that automate and protect through shrinking the attack surface, but they still do not address the core problem and thus, the security they do provide comes at a cost — a high degree of control friction that results in higher spending and new vulnerabilities.

Today the CIO, CISO, CTO, or IT Director can chart a bold new course of action by implementing automated controls, including a low degree of control friction, which predicts and prevents risk at all scales. By doing so, they deliver to the boardroom, employees, and customers what the AV industry has not been able to do in more than 30 years — a new mission, management model, and solutions that protect to enable unparalleled security for data, systems, business, and people.

## A New Reality

The new cybersecurity reality, where organizations gain greater agility and security with prediction and prevention, is not a change in degree, but a change in kind. The possibilities are far-reaching. Enterprises today can successfully use advances in automation, including artificial intelligence, machine learning, and big data, to secure like never before. Organizations need to embrace new capabilities to move forward beyond traditional AV and the detect and respond model. They should look at solutions that adapt and scale to cyber challenges as they emerge. At the core of these capabilities is 'the learning model', which departs from the core foundation of most security vendors today.

A learning system quickly predicts — and prevents — new threats. It also meets the demands of modern, mechanized attacks. The current technology landscape is a world of digital variation and frequency. IT staff cannot detect, respond, and plan for unknown challenges using the manual or semi-manual processes employed by traditional AV vendors.

The modern enterprise requires solutions that learn, adjust, scale, and process faster than manual and traditional solutions. If a threat gets past controls, organizations need to be able to learn as much as possible without compromising privacy. The extracted information enables precise, extensive investigation into what occurred. IT leaders can take proactive action that mitigates risk and vulnerabilities to prevent future attacks.

Learning systems, based on AI and machine learning, automatically analyze files, executables, and binaries to halt code before it executes and does harm. The modern application of AI and machine learning supply automated, preventative measures to stop more than for 99% of risks, including advanced persistent threats, malicious code, and zero-day attacks. You can successfully protect against both known and unknown attacks, without requiring a patient zero, whether its ransomware, zero-day threats, trojans, worms, or spyware. That means better threat protection, fewer alerts, more costs savings, reduced layers of control technology, and removal of control friction.

## The Business Case

When you protect to enable the mission using learning systems and the modern application of AI, you do more than provide agile risk management — you provide business value. You bring the strategic benefits of better cybersecurity to every corner of your organization.

- **Streamlined Operations:** Eliminate the need for EPP firewalls, device controls, host IPS, and anti-malware solutions
- **Reduce Incidents:** Decrease help desk tickets and refocus on strategic plans, including virtualization, cloud security, and IT automation
- **Improve Business Continuity:** Secure against attacks targeting your network, credentials, and data, while ensuring service to customers
- **Improve Compliance:** Meet government regulations and your internal security protocols with greater protection efficacy

## Conclusion

The 9 Box of Control concept helps model where an enterprise is with its security and where it could be, with automation and security fully integrated to change the speed and efficacy of protection. Most importantly, the concept — and the proposed change in philosophy from detect and respond to prevent and protect — elevates security to be fully integrated into your existing IT and business strategy. Why? Because it offers a different paradigm or worldview on risk management, where the upper right box is not the optimum place for the enterprise. In fact, it's the exact opposite — the lower left.

If an organization implements automated controls with a low degree of control friction that prevents risk, they deliver exactly what the AV industry has no incentive to develop — solutions and services that protect to enable people, data, and the business.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

CYLANCE™