

# KRAKEN EXECUTIVE REVIEW

INSIGHTS AND STRATEGIES FOR LEADERS  
BUILDING WHAT'S NEXT.

VOLUME 1 | ISSUE 2  
OCTOBER 2026

## The Business of Risk.

BUILDING ORGANIZATIONS THAT  
CAN WITHSTAND WHAT'S NEXT.



**LEADERSHIP**  
Who Really Owns  
Cybersecurity Risk?



**GOVERNANCE**  
The Decisions That  
Protect Enterprise Value



**RESILIENCE**  
When Technology Fails,  
Can Your Business Continue?



**EXECUTIVE PERSPECTIVE**  
Why Preparation Is a  
Competitive Advantage



**EXECUTIVE FOCUS**  
Clarity for Better  
Decision-Making



**OBJECTIVE INSIGHT**  
Data-Informed.  
Strategy-Driven.



**RISK AWARENESS**  
Understanding Today.  
Preparing for Tomorrow.



**FUTURE READY**  
Building Value That  
Lasts.

# Cybersecurity Is a Business Problem. Leadership Owns the Risk.

## Dear Fellow Leaders,

One of the most dangerous assumptions a business leader can make is that because someone is responsible for cybersecurity, the organization's cybersecurity risk is being managed.

Those are two very different things.

For years, businesses have approached cybersecurity primarily as a technology issue. We invest in security software, hire IT professionals, engage service providers, and implement technical safeguards. Those investments matter. They're essential. But they don't eliminate risk, and they certainly don't replace leadership.

## Cybersecurity is a business problem that happens to involve technology.

Consider what happens when an organization experiences a significant cyber incident. The immediate concern might be technical, but the consequences rarely stay there. Operations can grind to a halt. Employees may be unable to work. Customers may lose access to critical services. Revenue can disappear while expenses continue to accumulate. Contractual obligations, regulatory requirements, and reputational damage can complicate an already difficult situation.

And suddenly, the questions aren't technical anymore. How long can we afford to be down? Which operations must be restored first? What do we tell our customers? Who has the authority to make critical decisions? Those aren't questions your firewall can answer. They're leadership questions.

“ You can delegate the management of technology. You cannot delegate accountability for the risks facing your business. ”

## Risk Cannot Be Outsourced

Your technology team, cybersecurity professionals, and outside advisors play essential roles in identifying threats, evaluating vulnerabilities, implementing safeguards, and responding to incidents. But they cannot determine how much business risk your organization should accept. That responsibility belongs to leadership.

Effective cybersecurity governance begins when executives understand the relationship between their business objectives, operational dependencies, and the risks that could prevent them from succeeding. It means making informed decisions about priorities, investments, accountability, and resilience.

And it means recognizing that security isn't simply about preventing something bad from happening. It's also about ensuring your organization can withstand disruption, recover effectively, and continue moving forward.

## Building Organizations That Last

October is Cybersecurity Awareness Month, making this an appropriate time to revisit how we think about cybersecurity. But awareness alone isn't enough. We need organizations where leadership understands risk, employees understand their responsibilities, technology supports business objectives, and preparedness is part of the culture.

Because ultimately, the measure of a strong organization isn't whether it will ever face adversity. It's how prepared it is to respond when adversity arrives.

At Kraken Technology Solutions, we believe technology should advance the business. That philosophy extends to cybersecurity, governance, and operational resilience. Our role is to help leaders see the bigger picture, understand their options, and make better-informed decisions.

## The business owns the risk. Leadership owns the decisions. Technology helps execute the strategy.

Here's to building stronger organizations, making smarter decisions, and preparing for whatever comes next.

With gratitude,



*Steve Brickner*

**Steve Brickner**  
Founder & CEO  
Kraken Technology Solutions

## FEATURE STORY

# WHO OWNS THE RISK?

## Why Cybersecurity Cannot Be Delegated Entirely to IT

Technology professionals manage cybersecurity. But business leaders are accountable for the risk.

### A Question Every Leader Must Answer

Who is responsible for deciding how much cybersecurity risk our organization is willing to accept?

For many organizations, the answer isn't entirely clear. They have an IT department, may work with a managed service provider, employ cybersecurity professionals, carry cyber insurance, and invest in sophisticated security technologies. Those are important investments. But none of them changes a fundamental reality: **the organization owns its risk. Leadership is accountable for managing it.**

### Managing Security vs. Owning Risk

Cybersecurity professionals identify vulnerabilities, evaluate threats, implement controls, monitor systems, and respond to incidents. Their expertise helps reduce exposure.

But deciding whether a particular risk is acceptable requires understanding the business itself. Consider a company operating a critical system that cannot easily be taken offline for maintenance. The technology team may recommend immediate remediation. Operations may argue that shutting down the system would interrupt production and create substantial financial losses. Both perspectives may be valid. Ultimately, an authorized business leader must evaluate the competing risks and determine the appropriate course of action. **That's cybersecurity governance in action.**

### The Governance Gap

One of the most common challenges isn't a lack of cybersecurity technology. It's a lack of connection between technical activity and executive decision-making. Security reports describe vulnerabilities, alerts, and software updates. Executives need to understand what those findings mean for operations, financial performance, customers, compliance, and organizational objectives.

Closing that gap requires translating technical information into business risk. It also requires regular communication between leadership, technology professionals, and operational stakeholders.

### The Kraken Perspective

Effective cybersecurity governance doesn't require every executive to become a cybersecurity expert. It requires leaders to ask informed questions, establish clear expectations, and make deliberate decisions.

Technology professionals should provide the expertise. Leadership should provide the direction. And the organization should have a documented, repeatable process for understanding, treating, and monitoring risk.

**Because the goal isn't simply to build a more secure technology environment. It's to build a stronger business.**

“ Security professionals manage cybersecurity. Business leaders make the decisions that determine organizational risk. ”

## THE FIVE RESPONSIBILITIES OF LEADERSHIP



### 1. UNDERSTAND What Matters Most

Identify the business processes, systems, information, and relationships essential to your success.



### 2. ESTABLISH Risk Tolerance

Determine what levels of financial, operational, regulatory, and reputational exposure you are prepared to accept.



### 3. ASSIGN Accountability

Clearly establish who evaluates risks, recommends safeguards, authorizes decisions, and oversees implementation.



### 4. INVEST According to Priorities

Direct cybersecurity investments toward protecting critical operations and reducing meaningful business exposure.



### 5. VERIFY Control Effectiveness

Ask how you know your safeguards work. Expect meaningful reporting, testing, and evidence of effectiveness.

## EXECUTIVE INTELLIGENCE

# THE TRUE COST OF BUSINESS DISRUPTION

## Why Downtime Is More Than an IT Problem

When business leaders think about technology failures, they often think about the cost of getting systems back online. But the real financial impact of a disruption extends far beyond the technology itself.

Lost revenue. Idle employees. Missed deadlines. Interrupted customer service. Contractual penalties. Damaged relationships. And perhaps most importantly, opportunities that never return.

**The true cost of downtime isn't measured solely in hours. It's measured in business consequences.**

### THE RIPPLE EFFECT OF DISRUPTION

Imagine a growing company experiences a significant technology outage on a Monday morning. Its critical systems are unavailable. Employees cannot access essential information. Customers cannot place orders. Financial transactions are delayed. Leadership has limited visibility into what's happening.

By Tuesday, the organization is experiencing more than a technology problem. It's a business crisis. And every department is feeling the consequences.

### SIX AREAS OF BUSINESS IMPACT



#### OPERATIONS



- Interrupted production and service delivery
- Inability to access critical systems
- Delays across the supply chain



#### FINANCE



- Lost revenue
- Delayed payments
- Unexpected expenses
- Cash flow disruption



#### EMPLOYEES



- Idle time
- Reduced productivity
- Operational confusion
- Frustration and disengagement



#### CUSTOMERS



- Missed commitments
- Service interruptions
- Declining confidence
- Potential loss of customers



#### REPUTATION



- Damaged relationships
- Negative reviews and word of mouth
- Lost future opportunities
- Long-term brand impact



#### COMPLIANCE



- Potential contractual penalties
- Legal and regulatory consequences
- Reporting obligations
- Increased scrutiny

### THE QUESTIONS LEADERSHIP MUST ANSWER

#### 1 How long can we afford to be down?

Different business functions have different tolerance levels. A temporary interruption to an internal reporting system may be inconvenient. An outage affecting production, financial transactions, or customer-facing operations could be devastating. Leadership must determine acceptable downtime based on business impact.

#### 2 What information can we afford to lose?

Not all data carries the same operational value. Some information can be reconstructed. Other information may be difficult or impossible to replace. Understanding acceptable data loss helps establish appropriate recovery requirements.

#### 3 Have we actually tested our ability to recover?

Having backups does not automatically mean an organization can recover its operations. Recovery depends on technology, people, processes, vendors, communications, and coordinated decision-making. A recovery plan that has never been tested is still largely an assumption.

### THE KRAKEN PERSPECTIVE

#### Backups Protect Data. Resilience Protects the Business.

A backup is one component of a recovery strategy. True organizational resilience requires understanding critical business functions, identifying dependencies, establishing recovery priorities, assigning responsibilities, and validating that recovery capabilities work.

**The goal isn't simply to restore technology. The goal is to restore the business.**

### THE EXECUTIVE TAKEAWAY

**The question isn't whether your technology can be restored. It's whether your business can recover.**

Business continuity is a leadership responsibility supported by technology, people, and processes.

## EXECUTIVE PERSPECTIVE

# The Financial Side of Cyber Risk

## What Business Leaders Should Understand Before a Crisis

A cybersecurity incident can become a financial crisis long before the technology is fully restored. Understanding the financial implications of cyber risk is essential for making informed decisions, protecting your organization, and ensuring long-term resilience.

### 1. The Financial Exposure You Don't See

Most organizations understand the cost of cybersecurity software and IT services. Far fewer have calculated their potential financial exposure from a serious incident.

Consider the expenses that can accumulate:

- Incident investigation and forensic services
- Legal counsel and regulatory response
- Emergency technology restoration
- Business interruption and lost revenue
- Customer notification and remediation
- Contractual liabilities and penalties
- Reputational damage and customer attrition

Some costs are immediate. Others can continue affecting financial performance long after operations resume. The total financial impact often extends well beyond the initial incident response and technology recovery.

**Cyber risk isn't just a technology risk. It's a financial risk with real and lasting consequences.**

### 2. Cyber Insurance Is a Financial Tool, Not a Security Strategy

Cyber insurance can play an important role in managing financial exposure. However, policies vary significantly in their coverage, exclusions, conditions, limits, and deductibles. Business leaders should understand what their policies actually cover, what obligations they must satisfy, and how the claims process works.

**Having cyber insurance is not the same as having a financially resilient organization.**

Insurance can help transfer and mitigate financial risk, but it doesn't prevent incidents, eliminate operational disruption, or replace the need for strong governance, effective controls, and a well-tested recovery plan. Organizations should review their coverage with qualified insurance professionals.

### 3. The Questions Your CFO Should Be Asking

Cyber risk has direct financial implications, and CFOs play a critical role in understanding and managing that exposure. The right questions help ensure the organization is prepared, appropriately insured, and positioned to withstand a significant incident.

**These are financial governance questions, not technical troubleshooting questions.**

#### FOUR KEY FINANCIAL QUESTIONS FOR BUSINESS LEADERS



##### EXPOSURE

What would a significant cybersecurity incident cost our organization?

Understand the potential financial impact across operations, revenue, legal, regulatory, and reputational areas.



##### COVERAGE

Which financial consequences are covered by insurance, and which remain our responsibility?

Review coverage, exclusions, limits, deductibles, and claims obligations with qualified insurance professionals.



##### LIQUIDITY

Could we maintain essential financial obligations during an extended disruption?

Evaluate cash flow, access to capital, and financial resilience if revenue is interrupted.



##### INVESTMENT

Are we investing appropriately to reduce our most significant business risks?

Prioritize investments based on business impact, financial exposure, and organizational objectives.

## THE KRAKEN PERSPECTIVE

### Informed Investment. Greater Resilience. A Stronger Business.

Cybersecurity investments should be evaluated in the context of business risk, financial exposure, and organizational priorities. The objective isn't to spend as much as possible on security. It's to make informed investments that reduce meaningful exposure while supporting the organization's ability to operate, grow, and recover.

**The goal isn't simply to protect your technology. The goal is to protect your business.**

“The cost of cybersecurity is visible in your budget. The cost of inadequate preparation may not become visible until it's too late.”

## THE EXECUTIVE ACTION BRIEF

# Five Questions Every CEO Should Be Able to Answer

## A Practical Leadership Framework for Business Risk and Resilience

Strong organizations don't wait for a crisis to discover their weaknesses. They ask difficult questions, challenge assumptions, and make informed decisions before circumstances force their hand. Cybersecurity, business continuity, and organizational resilience aren't simply technology responsibilities. They're leadership responsibilities. And understanding where your organization stands begins with five questions.

01



### What Are Our Most Critical Business Operations?

**Understand what keeps your business running.**

Every organization depends on certain processes, people, systems, information, and external relationships. But have you identified which are truly essential? Leadership should understand which operations generate revenue, fulfill customer commitments, support regulatory obligations, and enable the organization to function.

#### EXECUTIVE ACTION:

Identify your five most critical business processes and the resources each depends upon.

02



### What Could Prevent Those Operations From Functioning?

**Understand your exposure.**

Cyberattacks aren't the only threats to business continuity. Technology failures, vendor outages, natural disasters, employee departures, supply chain interruptions, and operational mistakes can all disrupt an organization. The objective isn't to predict every possible event. It's to understand the vulnerabilities and dependencies that could create meaningful business consequences.

#### EXECUTIVE ACTION:

Identify the most significant threats and dependencies affecting your critical operations.

03



### How Long Can We Afford to Be Disrupted?

**Define your tolerance for downtime.**

Not every business function requires immediate restoration. Some can tolerate hours of disruption. Others may be unable to operate for even a short period without significant consequences. Leadership must establish acceptable downtime and data loss based on operational, financial, contractual, and regulatory requirements.

#### EXECUTIVE ACTION:

Establish recovery priorities and acceptable disruption thresholds for critical business functions.

04



### Who Makes the Decisions During a Crisis?

**Establish accountability before it's needed.**

During a significant incident, organizations may need to make difficult decisions quickly. Who can authorize emergency expenditures? Who determines whether operations should be suspended? Who communicates with customers, employees, insurers, regulators, and other stakeholders? Unclear authority creates delays, confusion, and unnecessary exposure.

#### EXECUTIVE ACTION:

Document decision-making authority, escalation procedures, and crisis communication responsibilities.

05



### Have We Actually Tested Our Assumptions?

**Confidence should be supported by evidence.**

Having cybersecurity tools, backups, policies, and recovery plans doesn't necessarily mean an organization is prepared. Plans must be tested. Employees must understand their responsibilities. Technology must function as expected. And leadership needs evidence that the organization can respond and recover.

#### EXECUTIVE ACTION:

Schedule a leadership-level tabletop exercise or business continuity review.



#### THE KRAKEN EXECUTIVE CHALLENGE

## BRING THESE FIVE QUESTIONS TO YOUR NEXT LEADERSHIP MEETING.

If your team cannot confidently answer them, you've identified an opportunity to strengthen your organization. You don't need to solve every problem in one meeting. Start by identifying what matters, understanding where you're exposed, and assigning responsibility for the next steps.

**Preparedness begins with leadership.**

“ Strong organizations aren't defined by the absence of risk. They're defined by how intentionally they prepare for it. ”

**STRONGER LEADERS. STRONGER BUSINESSES. STRONGER COMMUNITIES.**

Have an executive perspective worth sharing? The Kraken Executive Review welcomes contributions from business leaders and industry professionals.