Empowering the CFO

TOP 3 WAYS CFOS CAN MITIGATE CYBER RISK | CFO VANTAGE POINT

Real risks to business objectives

Cyber threats are real and present a material risk to your business. Protecting the company from these threats is no longer just the responsibility of the CIO and the CISO. Now, CFOs must play an active role.

To date, organizations globally are spending $100 billion annually on cybersecurity tools and services — and still losing the war. That figure is projected to jump to $170 billion by 2020.[1]

This is a problem that you can't afford to ignore. Are you ready?

$5.9 MILLION

The total average cost paid by organizations for each data breach in 2014.

PONEMON INSTITUTE

"2014 COST OF DATA BREACH STUDY"

1. "Worldwide cybersecurity market continues its upward trend," Steve Morgan, CSO Magazine, July 9, 2015.

Understand the risk

Many CFOs and finance leaders have taken a "see no evil" approach when it comes to cybersecurity. The subject matter is technical, complex and, at first glance, not the typical focus of the CFO. The threat landscape has changed. The risk to the business is clear, measurable and material.

How can the CFO calculate the risk? Ultimately, there are several considerations:

- Impact to your assets
- Impact to your reputation
- Types of vulnerabilities
- Types of attackers
- Company maturity to defend & respond

Each consideration has layers of variables that must be considered. What is the likelihood and cost of business interruption? Will brand damage impact a quarter or does it mean ongoing concern? Do you store regulatory data that is a target for threat actors? Do you have dedicated security operations? All of these factors have a significant impact on your cyber risk.

Understanding your cyber risk is an ongoing, cross-functional effort that must be refreshed as the considerations evolve. Risk-conscious companies have board-level support for continuing risk assessment.

"Understanding your cyber risk is an ongoing, cross-functional effort that must be refreshed as the considerations evolve."

Communicate & coordinate

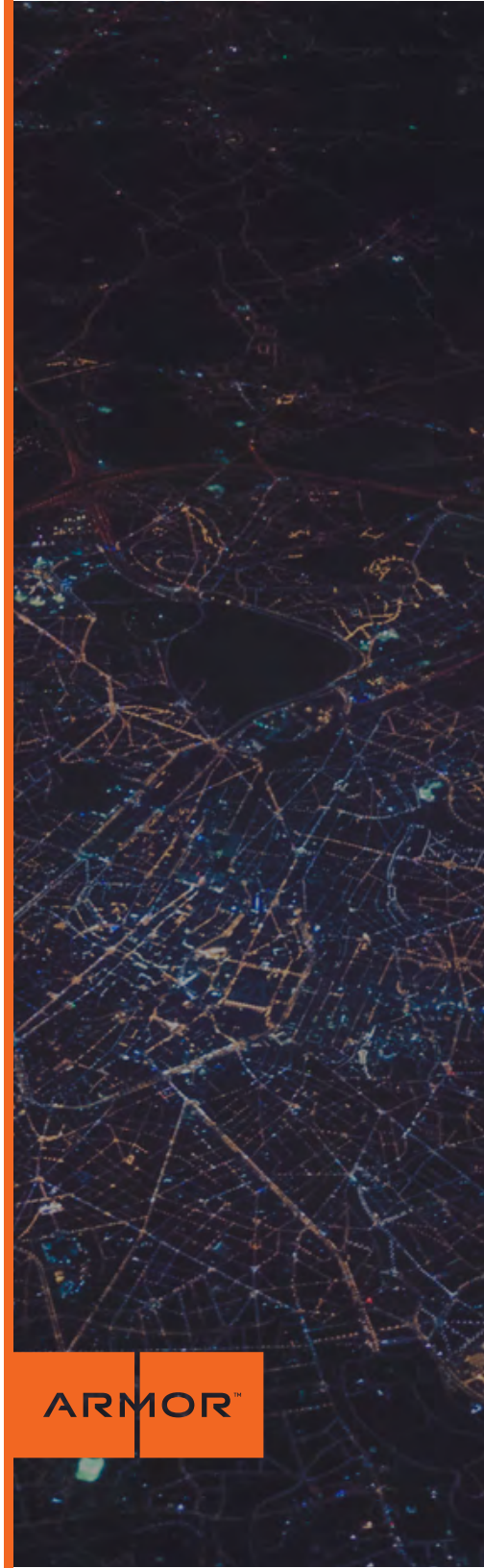
The CFO has the view of all required business outcomes, whether they are revenue-generating, focused on customer experience or complying with industry or regulatory requirements. The CFO has the tools through the budgeting, reporting and internal audit functions to ensure that cybersecurity priorities are being addressed.

The CFO's situation is unique. And their perspective is crucial. CFOs are aligned at the confluence of operations, compliance, legal, reporting and executive management. That lens allows the CFO a unique vantage point to direct all parties involved toward a security-focused strategy.

Recent litigation, directed at the boards of Target and Wyndham for breach of fiduciary duty relating to their recent data breaches, have leadership and stakeholders demanding clear and concise plans, controls, monitoring and reporting around cyber risk.

The CFO is often the primary conduit to the board of directors, ensuring the cybersecurity plans move from strategy to execution.

> "CFOs are aligned at the confluence of operations, compliance, legal, reporting and executive management."



Allocate the budget correctly

The most obvious action CFOs can take to mitigate cyber risk is through the power of the purse strings. Annual planning should consider departmental risk assessment, specific mitigation plans and the investment — capital and operating — are required to be secure.

While all functions have an obligation to contribute to a secure posture, special attention should be paid to the IT plans and needs. Aging legacy technology, custom applications, unmanaged use of the cloud and next-generation technologies (e.g., mobile, connected devices, etc.) will require significant spend to secure the applications, data and the business.

Sometimes, the cost of security may exceed the business value of a legacy application or system — creating a powerful opportunity to improve both the business execution and the security posture.

CFOs should also utilize external resources where possible. The costs of staffing, training and retaining an effective security operations center (SOC), for example, is prohibitive for all but the largest and most sophisticated enterprises; as are the myriad of new security tools released everyday.

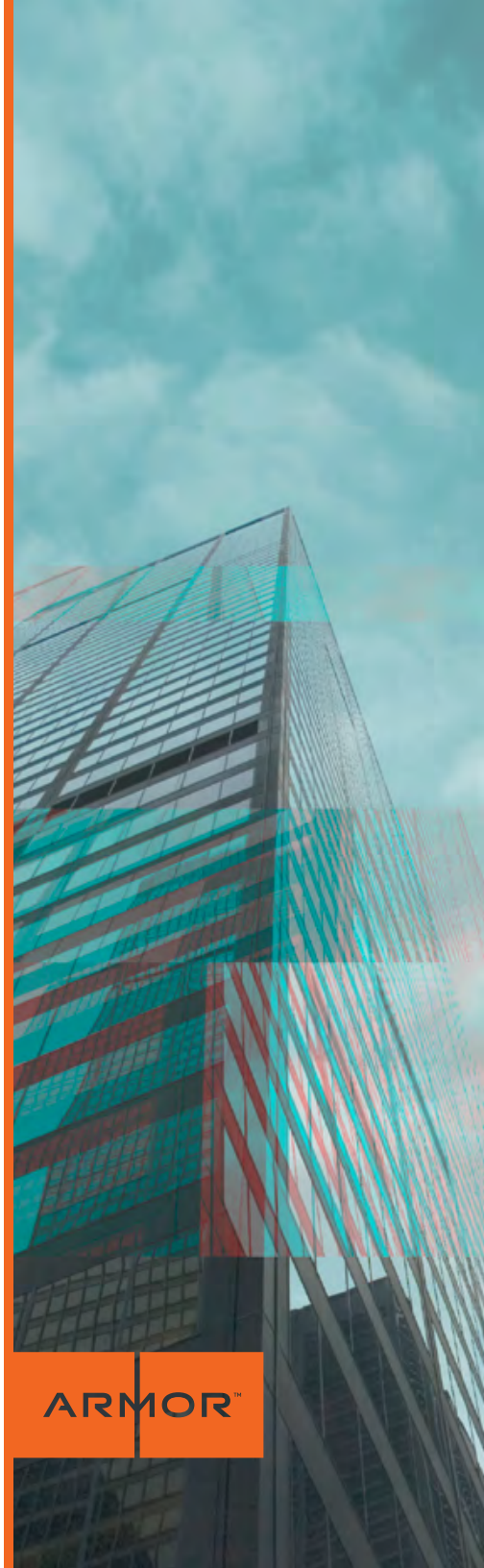
Resist the temptation to chase the latest and greatest. New technology requires significant integration, management and tuning, and must be combined with intelligence capabilities in order to deliver the maximum value.

Unless your business can achieve a significant, defensible differentiation from building and owning a significant security operation, consider outsourcing. You will achieve stronger and more effective outcomes for less.

"29% of organizations are unable to meet cybersecurity objectives as a result of budget constraints."

GRANT THORNTON

"THE CFO'S ROLE IN CYBERSECURITY" | JUNE 2015



US 2360 Campbell Creek Boulevard, Suite 525, Richardson, Texas 75082 | Phone: +1 877 262 3473
UK 268 Bath Road, Slough, Berkshire SL1 4AX | Phone: +44 800 500 3167