Secureworks®

WHITE PAPER

Protecting Your Profits

The New Economics of Cybersecurity and Its Four Best Practices

Digital transformation has made cybersecurity one of the world's most pressing issues at both the micro and macro levels. At the micro level, organizations face existential consequences from a severe breach—regardless of how well they execute in every other area of the business. At the macro level, the digital economy is unsustainable if it is constantly subject to disruption by malicious actors.

In response to this intense demand for cybersecurity, capital markets have made massive investments in cybersecurity technology, services, research, and skilling. And those investments have paid off, greatly enhancing the abilities of both individual organizations and collective markets to protect themselves from an ever-intensifying threat matrix.

Unfortunately, the way many business leaders think about the economics of cybersecurity remains seriously problematic. While the case for and value of strong cybersecurity and bold cybersecurity investments has been proven time and after time, still many executives are fighting a deeply held belief that cybersecurity is a cost center. There's a mentality that cybersecurity means you're paying for (hopefully) nothing to happen. But this misconception couldn't be more wrong.

How much is it worth to protect your other investments, your resources, your employees, and your customers? When the return is that your business gets to continue growing and expanding, the idea of ROI can suddenly seem very different when it comes to cybersecurity. Now you're investing in mitigation of risk, regulatory compliance, customer confidence, brand value, and priceless global security in our digital economy. So it cybersecurity a cost center? Or is it necessary to protect every profit center you have?

Cybersecurity success therefore requires more than just technology, services, research, and skilling. It also needs rationalized economics. It also needs rationalized economics - and soon.

No organization can appropriately prioritize its investments in cybersecurity without such economics. Nor can it accurately assess the efficacy of those investments to continuously optimize funding of its evolving cybersecurity imperatives.

It is time for organizations to add rationalized cybersecurity economics to their short lists of cybersecurity necessities.

Cybersecurity, after all, is practiced in the same financial universe as R&D, marketing, sourcing, pricing, compensation, M&A, and capital management. Economic rationality is as vital for effective cybersecurity as it is for every other business endeavor.

And for that economic rationality to have positive impact on an organization, it must be operationalized. An economically rationalized approach to cybersecurity is, in fact, a must for every organization that will successfully compete in the digitally transformed global markets of the 21st century.

Cybersecurity spending buys global security in the digital economy.

"There's a mentality that cybersecurity means you're paying for (hopefully) nothing to happen. But this misconception couldn't be more wrong."

Paying for Nothing: A Brief History

Once upon a time, organizations did not need rationalized cybersecurity economics. They simply deployed a firewall and installed some antivirus software. Neither one cost much and both were easy to manage.

Then things got more complex. Organizations built more extensive IT environments that touched more areas of the business. Application and operating system code grew in scale and complexity, creating exponentially greater potential for software vulnerabilities as it did so. Workloads shifted from on-premises to clouds. Workforces began shifting to hybrid—and then, during the global pandemic—fully remote work environments, vanishing the "perimeter." Through it all, those increasingly complex environments became more so as they linked to suppliers, partners, customers, and the global Internet.

These quantum increases in cyberthreat surfaces drove increased cybersecurity defensive requirements. But most organizations at first resisted commensurate increases in cybersecurity spending. It was only after a combination of high-profile breaches, privately experienced business trauma, and years of passionate exhortation by cybersecurity advocates, that organizations began to understand the urgent need for enlarging their cybersecurity budgets.

According to Forrester, global cybersecurity budgets have been growing at the healthy clip of 16% year over year since 2018. That is not a bad number, but it begs new questions, including:

- Is 16% annually enough to make up for past underfunding?
- Is the risk posed by cyberthreats increasing by more than 16% annually? If so, should cybersecurity funding reflect that?
- Does the size of the budget that an organization explicitly allocates to cybersecurity staffing, tools, and services accurately reflect its true security spending?
- How are cybersecurity budgets being suballocated? Is that suballocation really optimal?
- How can organizations intelligently benchmark the financial performance of their cybersecurity investments against the performance of other corporate organizations?
- How can organizations continuously improve the financial performance of their cybersecurity investments over time—especially as more and more dollars are at stake?

$20B

Cost of ransomware payments in 2020[1]

80%

Successful breaches are new or unknown[2]

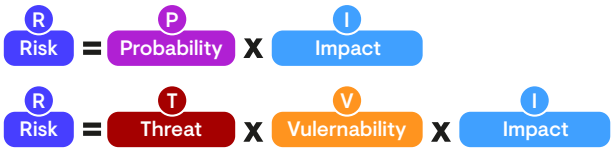
Quantum increases in cyberthreat surfaces drove increased cybersecurity defensive requirements.

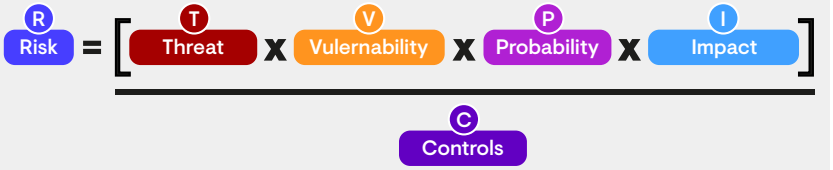
[1] Cyber Security Trends 2021

[2] Ponemon Institute, The Third Annual Ponemon Institute Study on the State of Endpoint Security Risk, 2020

Secureworks®

It is time for cybersecurity spending to become further rationalized. And some great thinkers have worked to translate cybersecurity risk into currency-quantified metrics using formulae, for example:





Sadly, these formulae have fallen short of the mark for many reasons. As in the above example, most variables are difficult to quantify due to a lack of objective data. As well, the volume, variety, variability, and velocity of risk exposures that organizations face make it impractical to perform these calculations in the real world at scale in a timely way. And these metrics may simply be too difficult to capture, causing a calculation to require more resources than it could potentially save.

While the formulae such as the one above are useful in concept, they do not yield the practical guidance organizations need to rationalize cybersecurity budget allocations. That is why allocations continue to be based mostly on educated guesses and gut feeling.

This status quo is unacceptable if organizations are to properly defend against ever growing cyber threats and IT landscapes that are continuing to expand in size and complexity. There is simply too much at stake at both the micro and macro levels. And the odds are stacked against them.

$2B Organizations paid $2B to **ransomware** perpetrators in 2021.

80% 80% of successful **breaches** result from threats that are new or unknown to cybersecurity teams.

↑ 50% **Known vulnerabilities** jumped 50% from 2019 to 2020 due to changes in how organizations implement technology, including big moves to remote computing, BYOD, and the cloud.

2.7M The global **shortfall in qualified security professionals** is now about 2.7 million human beings.

... allocations continue to be based mostly on educated guesses and gut feel.

... cybersecurity stakeholders—perhaps most importantly including CFOs and other resource allocation leaders—need a better basis for their financial cybersecurity judgements and decisions.

Forrester's average 16% budget increase may be enough to address these escalating conditions. Or it may not. Either way, cybersecurity stakeholders—perhaps most importantly including CFOs and other resource allocation leaders—need a better basis for their financial cybersecurity judgments and decisions.

"Phase Three" Cybersecurity Economics: Goals-Driven Resourcing

The preceding historical review is useful because the past is prologue. To understand what the next phase in cybersecurity economics requires, look back at the previous two phases.

PHASE 1

In the **first phase** of cybersecurity economics, organizations saw themselves as **paying for nothing**. Cybersecurity spending was trivial, and thus required little serious examination.

PHASE 2

In the **second phase**, organizations saw themselves as **paying for something bad not to happen**. Cybersecurity budgets grew morea significant, and thus required some level of accountability.

PHASE 3

Now, in the **third phase** of cybersecurity economics, organizations must understand that they are paying for something of great value: **the ability to achieve their goals** by aggressively driving digital transformation with the utmost confidence and true operational excellence.

These are the characteristics of organizations experiencing the third phase of cybersecurity economics.

- Investments in cybersecurity must **grow to the level that is truly necessary** to support its strategic goals. No more assumptions or budgetary math based on prior year spending.
- Given the likely scale of these investments once properly established, **true financial discipline and stewardship** of cybersecurity budget allocations becomes a necessity with Board-level visibility.
- Organizations must view their investments in cybersecurity **as fundamentals —more like payroll, R&D, and CapEx spending— rather than as siloed, discrete budget allocations.**

This transition from paying for ***nothing*** to happen (defense) to paying for ***something*** to happen (success) must not be minimized. The rationalization of cybersecurity economics requires new and better technology, formulae, and best practices. But, first and foremost, third-phase cybersecurity economics requires executive leadership to reframe the value of cybersecurity at its most fundamental level.

Until this happens, organizations remain stuck in obsolete funding models and operational practices. And for them, it gets worse. Those that fail to adapt to the new model are more vulnerable to cyberthreats than those that do. And while those that embrace the new model can justify their cybersecurity spending at the right levels, those that fail to do so will remain underfunded and under protected—just as cyberthreats are growing in number, complexity, and severity.

When 16% is not enough, it is time to reframe your cybersecurity funding. Here is a way for organizational leaders to conceptualize a new approach.

PHASE 1	PHASE 2	PHASE 3
"Cybersecurity is kind of a tax we pay for owning technology."	"Cybersecurity is a necessary cost of doing business."	"Our cybersecurity investments empower us to confidently achieve our strategic goals."
"Cybersecurity spending is a minor IT department issue."	"Nothing bad happened to us, so we must be appropriately resourcing cybersecurity."	"We are aggressive about both funding cybersecurity and getting the most for our spend."
"Our cybersecurity costs are firewalls, antivirus, and authentication/authorization."	"Our cybersecurity spend includes a full portfolio of technologies, services, and SecOps staff."	"SecOps is just one component of our organization-wide commitment to cybersecurity."

To many, the Phase 3 approach to re-framing cybersecurity economics may seem intuitively obvious. Taking this approach is essential to digital transformation, it means getting the greatest possible value from cybersecurity investments, and it enables an organization to aggressively leverage technology to delight customers, drive down costs, respond more nimbly to change, and impress investors.

In practice, however, many organizations remain conservative, reactive, and inadequately disciplined when it comes to resourcing cybersecurity. That is not a formula for success in the age of digital transformation and disruption.

18K

Vulnerabilities in 2020, up from 12k in 2019[3]

2.7M

Global Shortage of Cybersecurity Experts[4]

Four Best Practices for Operationalizing Next-Gen Cybersecurity Economics

How can executive and cybersecurity leaders operationalize a Phase 3 view of cybersecurity economics? Here are four best practices—each expressed in the form of a question—that align with cybersecurity as a strategic enabler of the business, rather than a profit-eroding cost.

1. What do we need?

Cybersecurity budgets are calculated as a percentage of some other number, such as a fraction of IT infrastructure spending or a fixed increase from last year's budget. To make the transition to third-phase economics, budget decisionmakers must take a fresh look at their cybersecurity allocations:

Security controls for current and near-term digital transformations.
As an example, organizations that have not implemented multi-factor authentication in the past probably will not be able to do so this year if they are restricted by an inadequate budget. Similarly, organizations that chronically lag on patching tasks will forever be playing catch-up—an extremely dangerous game—if they do not allocate sufficient resources to address both their current and near-term projected vulnerabilities.

A fresh, complete inventory and gap analysis should be on every organization's agenda for 2022. This baseline can then be built upon for inventories and gap analyses in future years.

Ongoing access to robust, up-to-date threat intelligence.
As noted above, new threats—in the form of new attacker exploits and reports of software vulnerabilities—emerge at a much faster pace than ever before. SecOps teams cannot effectively protect their organizations without continuous access to this intelligence. Next-generation resourcing demands that organizations incorporate the cost of this intelligence into their cybersecurity budgets.

[3] SC Magazine Article from Redscan Report.
[4] Infosecurity Magazine from (ISC)² Cybersecurity Workforce Study

SecOps staff scale and skilling assessment.
Organizations cannot safely pursue digital transformation with cybersecurity technology alone. People—smart, skilled, motivated, and experienced people equipped with the right technology and intelligence—are ultimately what protect an organization from those who would do it harm. But there is an extreme shortfall in the number of such people available to the organizations that need them. This is where services like managed detection and response (MDR) can make a great impact. Now organizations who do not wish to maintain a 24x7 SoC can extend their capabilities and manage the pressure to continually hire and retain talent.

Opportunities for engagement with external security solution providers.
The challenges of cybersecurity in the 21st century are well beyond the capacity of even the largest organizations in the world to address alone. Every organization should re-calibrate the role that outside service providers play in their digital transformation strategies. Potential service engagements range from periodic adversarial testing and vulnerability assessments to ongoing SecOps and emergency response support. The cost savings they offer are due to a variety of factors—including economics of scale and avoidance of long-term fixed overhead.

Special care should be taken to ensure that services are engaged appropriately (and, as may often be the case, temporarily) as part of any major expansion of an organization's digital footprint—whether that expansion involves M&A, entry into new geographic markets, or any other initiative that may be a reach too far for its internal SecOps team.

2. Where and how can we optimize our investments?

As cybersecurity allocations increase, it will become more important than ever to ensure that they are applied with maximum effect and minimum waste.

Automation and machine learning.
Technology can never fully supplant human intelligence in cybersecurity. It can, however, magnify staff productivity by automating routine tasks, accelerating staff responsiveness, and ensuring that staff efforts are intelligently prioritized based on actual needs of and risks to the business.

One area where machine learning and automation show great promise is in vulnerability management solutions that combine security analytics with human intelligence. Few organizations can instantly patch every common vulnerability and exposure (CVE) the moment it is first reported. New algorithmic techniques that correlate CVEs with actual risk to an organization based on its infrastructure and digital architecture are a much smarter way of prioritizing patching activities.

Future-proofing broad and deep threat detection.
Organizations are exploring extended detection and response (XDR) because they want a single solution to ingest data from their wide range of telemetry sources (cloud, network, endpoint, email, identity, etc.), and then apply analytics and human intelligence to detect threats and prioritize the greatest risks. XDR platforms maximize existing data. With no need to rip and replace, organizations can instead rely on a holistic, intelligent view of their existing telemetry to inform and alert their cyber defenses.

Do-or-buy decision-making.
Escalating demands on corporate SecOps teams are drive growth in the cybersecurity services market. These services give cybersecurity leaders options when it comes to what should be done by in-house staff and what can be more cost-efficiently done by outside vendors. Vendors also present opportunities for transfers of expertise to internal resources—which represents significant economic value given the urgent need to upskill existing SecOps staff.

Retrospective analysis of operational efficiency.
In re-thinking the economics of cybersecurity, organizations should consider ways to retrospectively assess how efficiently they perform key tasks. SecOps teams have not typically been subject to this type of analysis since their main success metric has been whether they were able to protect the organization from threat actors. Going forward, cybersecurity decision-makers should expand their evaluations of SecOps performance to look more aggressively to better align SecOps team behaviors with the organization's top goals.

One area where the machine learning and automation show great promise is in vulnerability management solutions that combine security analytics with human intelligence.

3. How can we make our organization more secure?

In the first two phases of cybersecurity economics, SecOps teams have functioned primarily as a siloed discipline, taking sole ownership of cybersecurity-related risks. But with third-phase economics, where cybersecurity is treated as a strategic imperative for the organization as a whole, that silo must be smashed. An ounce of cybersecurity prevention will deliver more bang for the buck than many pounds of SecOps cure. That's why organizations should take all the measures necessary to shift the burden of risk mitigation from higher-cost SecOps cures to lower-cost preventive measures, such as:

Building for cybersecurity.
The SecOps burden can be lightened if an organization's other technology teams—most notably IT Ops, application development (DevOps), and data management (DataOps)—build for security. DevOps, for example, can use testing tools to discover potential vulnerabilities in their code early in the development lifecycle, while they are still easy to fix. DataOps can aid risk mitigation through data masking and encryption.

Security is almost never included in the performance KPIs of other teams—and that omission must be remedied. These teams must have the technology, people, and processes necessary for them to contribute to the total cyber-confidence of the organization.

Employee training and practices.
Every chain is only as strong as its weakest link. At most organizations, people are the weakest links in the cybersecurity chain. This is especially true as malicious actors become ever more adept at leveraging readily available personal data to engage in social engineering, phishing, spear phishing, trojans, worms, bots, spyware, clickjacking, and even more exploits—as well as those yet to be developed.

Under second-phase economics, security-related training for technology end-users has generally been insufficient—in large part due to the understanding that SecOps would and/or should be able to clean up any mess created by someone opening the wrong email, clicking a bad link, or using a weak password. Under the third-phase model, this faulty economic reasoning no longer applies. The investments that individual departments and HR make in rigorous security-related training are as exactly that: investments that support achievement of strategic goals, rather than annoyingly burdensome costs.

Also, under second-phase economics, the security policies and practices that protect the interests of the organization have been insufficiently stringent—since convenience and productivity are superseding values when security is seen exclusively as a cost. Third-phase organizations certainly do not want to create counterproductive difficulties for users. But they are much more likely to pay a relatively small price for cyber safety on the front end to avoid a much higher price on the back end.

... teams must also be resourced with the technology, people, and processes necessary for them to contribute to the total cyber-confidence of the organization.

Securing the ecosystem.
Finding suppliers and partners who can deliver the right stuff with the right quality at the right price at the right time is hard enough. Burdening those relationships with stringent cybersecurity requirements only makes life harder for procurement and business relationship managers.

Under a third-phase model for cybersecurity economics, those requirements are a strategic investment rather than a burden. It does no good for an organization to save 8% on a million-dollar contract if the cheaper supplier then exposes it to a multi-million-dollar security breach.

As more organizations have come to recognize the risks and costs of breaches, the market has responded with more and better ways to assess the cybersecurity posture of potential partners: hence the advent of cybersecurity insurance and new processes and resources in place for the explicit purpose of managing the costs of cybersecurity insurance premiums. Third-phase organizations will take advantage of these solutions as part of their overall effort to trade pounds of cure for ounces of prevention.

... hence the advent of cybersecurity insurance and new processes and resources that they are put in place for the explicit purpose of managing the costs of cypersecurity insurance premiums.

4. How will executives lead?

In the first and second phases of cybersecurity economics, executive management took little or no responsibility for cybersecurity. With the advent of third-phase economics, that changes. *But how?*

Executives do not write marketing email messages or give front-line customer service staff their performance reviews. But they do make executive-level decision about marketing and customer service that set the tone for those emails and performance reviews.

Similarly, if an organization is engaged in digital transformation, that organization's executive must exercise reasonable leadership over organization-wide cybersecurity efforts that ensure the organization's ability to pursue its strategic goals with the necessary excellence and efficiency of execution. This includes:

Re-framing cybersecurity as a strategic imperative.
Employees generally do not assume appropriate responsibility for achieving optimum cyber safety at minimum cost unless that cause is championed at an executive level. At least some of that championing must be done at the very highest level of the organization.

Every executive has their own management style. So, third-phase cybersecurity leadership can manifest in many ways. But it must be visible, and it must insist on accountability. Otherwise, cultural inertia will set in—and cybersecurity will get backburnered as a mere cost that is the sole responsibility of the specialists in SecOps.

Avoid, mitigate, transfer, or accept.
Risk tolerances vary significantly from organization to organization. For some, risk is nearly intolerable. For others, high risk is intrinsic to the pursuit of high reward. Risk tolerance levels need to be set at the highest level of an organization—and then propagated across the chain of command.

Along with risk tolerances go risk management strategies and tactics. Here, too, executive leadership is indispensable. Organizations with low tolerance for risk may have to avoid risk altogether by passing on certain opportunities. In other cases, organizations will choose to mitigate risk—which is where cybersecurity and cybersecurity economics come in. Executives can also decide where it is appropriate to transfer risk through cyber insurance or contractual provisions.

Finally, executives determine where and when it is appropriate to accept a certain degree of risk. No organization has an infinite budget for cybersecurity—so it is logistically impossible to engage in digital transformation with zero risk of digital compromise. That is a call that executives must make on an informed basis, applying the principles of third-phase cybersecurity economics.

Crisis and continuity planning.
To accept risk means accepting the consequences when risk becomes reality. Executives must ensure that their organization is fully prepared for potential cybersecurity breaches. This should include periodic full-scale tabletop rehearsals of crisis and continuity scenarios to test the viability of scenario plans.

These rehearsals do more than prepare an organization for disaster. They also help managers come to terms with the real scale of the risks that the organization is accepting—which in turn helps organizational leadership reassess risk tolerances and increase investments in risk mitigation.

These four questions and their associated bullets are not intended as an exhaustive description of everything an organization must do in the 21st century to align its cybersecurity resourcing with strategic goals. It highlights how a third-phase perspective on cybersecurity economics—embracing cybersecurity as a complete set of best practices that serve as an essential investment in success, rather than as a silo of defensive costs—impacts organizations horizontally across all functions and vertically across all levels of leadership.

Cybersecurity has become too important to be left entirely to cybersecurity professionals.

Executive Conversations for the First Cybercentury

Cybersecurity is no longer an ancillary business function. It is as intrinsic to business in the new century as any other discipline, if not more so. Organizations must therefore reframe and rethink the way they resource cybersecurity—and the way they exercise stewardship of those resources.

Cybersecurity is too important to be left entirely to cybersecurity professionals. So, while SecOps teams must make the most of the resources they are given, executives cannot allow the fate of the organizations they lead to depend entirely on how well those teams stretch those resources.

Instead, executive leadership must work with SecOps to right size cybersecurity resourcing, promote organization-wide behaviors that support cybersecurity imperatives, and better align cybersecurity efforts with the actual goals of the organization—especially as those efforts relate to digital transformation, business expansion, financial performance, brand value, and tolerance for risk.

Because cybersecurity is no longer about paying for nothing. It is about making the investments necessary to thrive in a digital world fraught with dangers that not only threaten us individually—but also threaten human progress.

Calculating cybersecurity value

Organizations have tried a variety of formulae for calculating risk in financial terms. Under third-phase economics, organizations must evolve to frame cybersecurity allocations as investments necessary to achieve their strategic goals. Here are three ideas to consider from a mathematical perspective:

Cybersecurity value should be calculated using a formula like that used for other aspects of the business.
These methods vary. Some organizations still use the basic formula ROI = Return (R) / Cost (C) or, where appropriate, [Final Value (FV) – Initial Value (IV)] / Cost (C). Others use formulae such as Net Present Value (NPV) and Internal Rate of Return (IRR).

Cybersecurity value calculations should include a factor that reflects risk-based contributions to business objectives.
An organization spending $X to add five new distribution facilities that use the same IT infrastructure as existing ones takes on little additional cybersecurity risk. On the other hand, an organization spending the same $X to add a new set of customer-facing data access features to its mobile app may take on significant additional risk. Value calculations should reflect this difference. For example, an NPV-based calculation might look like this:

$$\text{Cybersecurity NPV} = \left[\sum_{t=1}^{n} \frac{Rt}{(1+i)^t}\right] x\,\mathrm{F}$$

Rt = net cash inflow-outflow during period t,

i = the discount rate or return that could be earned in alternative investments,

n = the number of time periods,

and F = the risk-based contribution factor of cybersecurity on a scale from 0 to 1.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111 00971
4 420 7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp