proofpoint.

E-BOOK

The Cost of 'Good Enough' Security

Calculating the true value of cybersecurity solutions

Cyber Crime and Business Risk

Whoever said crime doesn't pay apparently didn't anticipate modern cyber attacks. The average cost of a data breach to affected U.S. businesses grew from $5.4 million in 2013 to $9.44 million in 2022[1]—well outpacing inflation over the same period. Collectively, data breaches cost U.S. businesses about $1.4 billion per year. This adds up to $5,400 for every American adult.[2]

On a global scale, cyber crime is forecast to cost the world $10.5 trillion per year by 2025.[3] Other researchers estimate that cyber crime costs businesses an incredible $1.79 million every *minute*.[4]

Clearly, these costs are enormous. But they don't stop at the immediate financial losses. Cyber crime can damage your business's reputation or lead you to incur fines from regulators. It can disrupt operations and even derail your business model, making it impossible to follow your core strategy.

There's no way to entirely avoid the risks associated with cyber crime. They're simply part of what it means to do business in today's world.

However, it is possible to manage these risks. Just as business leaders and risk management officers plan and prepare for other risks that are implicit in doing business, you can limit your exposure to cyber crime risk. As with other types of business risk, you'll need to model the financial losses that a cyber attack might cause your business. Then you can make a plan for how to balance those risks against what it would cost to reduce them.

Globally, the average cost of a data breach is now up to **$4.24 million.**[5]

Experts forecast that cyber crime will cost the world **$10.5 trillion**[6]

One percent of the world's GDP is now lost to cyber crime.[7]

Cyber crime costs businesses **$1.79 million** per minute.

1 IBM. "**Cost of Data Breach Report 2022.**" July 2022.
2 Rick Newman *(Yahoo Finance)*. "**We're all paying a cybersecurity tax.**" May 2021.
3 Steve Morgan *(Cybersecurity Ventures)*. "**Cybercrime to Cost the World $10.5 Trillion Annually by 2025.**" November 2020.
4 James Coker *(Infosecurity Magazine)*. "**Cybercrime Costs Organizations Nearly $1.79 Million Per Minute.**" July 2021.
5 IBM. "**Cost of Data Breach Report 2022.**" July 2022.
6 Steve Morgan *(Cybersecurity Ventures)*. "**Cybercrime to Cost the World $10.5 Trillion Annually by 2025.**" November 2020.
7 Zhanna Malekos Smith and Eugenia Lostri *(Centre for Strategic and International Studies)*. "**The Hidden Cost of Cybercrime: Report.**" December 2020.

The first step in evaluating solutions is to compare a solution's risk resistance with its costs, to be sure you are getting the best value for your money.

Investing in security technologies is one strategy for reducing these risks. But how can you be confident that the investments you're making are the wisest ones?

As a CISO, risk reduction is your primary goal. The first step in evaluating solutions is to compare a solution's risk resistance with its costs, to be sure you are getting the best value for your money. You should also be sure to factor in costs beyond licensing, such as hardware, deployment, operability and ongoing maintenance costs. And consider additional benefits solutions may offer, such as workforce efficiency.

Let's take strain on your internal security staff as an example. Today's CISOs are grappling with staffing shortages in their security operations programmes. Globally, 2.72 million cybersecurity positions remain unfilled.[8] It's estimated that the cybersecurity workforce would need to grow by 65% to effectively defend organisations' critical assets.[9] For CISOs, these challenges are a day-to-day reality.

It's clear that security professionals' time is valuable and administrative overhead must be considered among the costs of a cybersecurity solution. But what about end user productivity? Or the labour costs associated with incident response? Or those of reporting on an incident?

In this guide, we'll take a closer look at the costs associated with deploying–and running–a cybersecurity solution. We'll take a deep dive into all the factors that can determine the total value of a solution, including some you may not have considered. We'll calculate when it might be more cost-effective to invest in an advanced email security solution or a complete email and cloud threat protection solution than it is to go with "low-cost" add-on capabilities or legacy solutions.

8 (ISC)2. "**Cybersecurity Workforce Study.**" March 2022.
9 Ibid.

Managing Cybersecurity Risk: the True Costs

Your investments in cybersecurity are certainly a means of buying down operational and business risk. But it's not simply a one-to-one relationship between dollars spent and depth of coverage. You need a layered security approach for solid defence.

Some security solutions will reduce your risks more than others. Small differences in efficacy can have a big impact on the risk—and potential cost—of a breach. Nor are all solutions' prices the same.

It's crucial to factor all these elements into your purchasing decision. This means taking your potential total return on security investment (ROSI) into consideration.

To do so, you'll need to think about all the losses that would come with a major breach event. These go far beyond the costs associated with the breach itself. Long-term damage to the business and its reputation may have an impact for years afterward.

Against these possible losses, you will need to balance the cost of the cybersecurity solution itself. At first glance, this may seem like it would be easy to calculate: just look at the licensing fees.

But when it comes to the total economic value of a cybersecurity solution, licensing costs are just the tip of the iceberg. If you are only looking at licensing, you are not seeing the full picture of what a solution will cost your organisation. Many other hidden costs of ownership lurk beneath the surface and can dramatically increase the overall cost of a solution.

And risk reduction is not always so straightforward. Leveraging the full capabilities of a solution may reduce your risk by 50%, but rarely are you able to take advantage of all of a product's capabilities right away. And most solutions offer benefits beyond risk reduction, including security team efficiencies, that increase the solution's value.

The aftereffects of a breach

Breach-related losses can include some or all of the following:

- Lost business and customers
- Lost data as well as the loss of the value to be gained from analysing that data
- Direct financial losses*
- Reputational damage
- Lost employee productivity
- Operational downtime
- Decreased share value
- Lost intellectual property
- Lost competitive advantage
- Compliance penalties or fines

* These can include ransom payments and the costs of labour and service for incident response and recovery.

Adding up the costs

For most organisations, adopting a new cybersecurity solution can be expensive and time consuming. The process can also be disruptive to users, regular IT and security operations. Some tools are cumbersome to maintain, increasing the burden on already-busy security teams. To estimate the total financial impact that the purchase will have on your organisation, you'll need to consider several factors:

Licensing

What do you pay the vendor annually per user for the solution? Your total licensing cost is the cost per user per year multiplied by the number of users.

Hardware

Some solutions can also involve hardware, which also adds cost(s) for your organisation. That can be especially true if you are managing that hardware on premises. What will it cost you to keep this hardware up to date, maintain connectivity, maintain the proper facilities, or prepare and recover from disasters? How many of your employees will maintain the equipment?

Ongoing Management

You can think of ongoing management costs as the time spent by specialist employees to support ongoing management activities. This factor is important to consider. Imagine that one solution takes two full-time employees to manage and another one requires only one. You would need to account for the fact that ongoing management will cost twice as much over the long term for the first solution. When you're looking at it this way, a solution that's ostensibly "free" can quickly become much more costly than a paid-for product that's easy to administer. This especially true if that product's vendor backs it up with strong support.

Deployment

Professional services
Many vendors will recommend or even require their professional services team to help you set up and deploy the solution. These services, of course, come at a cost.

Resource time
Whether or not the vendor's professional services team is involved, new product deployments also require at least some work from your internal employees. How many of their hours will this project take? From whom? Estimating the number of labour-hours from your salaried employees is only the first step. What other responsibilities will they need to set aside to focus on this initiative? You will also need to think about what you might lose if professionals aren't doing other high-value work.

Digging deeper into the total costs of ownership of a cybersecurity solution, it soon becomes clear that implementation and ongoing maintenance costs can outweigh the expences associated with licensing.

Consider the benefits

To understand the total value of a solution, consider all the costs above and weigh them against the benefits the product offers. Risk resistance is certainly the primary benefit of any security solution. But as with costs, there are other factors to consider as well.

Here are the benefits you should keep in mind:

- **Risk resistance**

  To calculate the risk resistance of a solution, you first need to understand the potential loss magnitude for your organisation. What is the average cost of a data breach in your industry and region, and for a company of your size? You will need to weigh this against your vulnerability and the solution's risk strength. Finally, consider that it may take some time for you to ramp up a solution and take advantage of its full benefits.

- **Workforce efficiency**

  User productivity
  Productivity can take many forms. But the two that are most important for security leaders are the productivity of the user base as a whole and the productivity of your security and IT teams. A cybersecurity solution can affect the productivity of employees in various, complicated ways. These effects extend to end users as well as cybersecurity and IT teams. How many minutes or hours of a business analyst's time would be lost if they didn't have access to their laptop while malware was being scrubbed from the device, for instance? How much would it cost your enterprise if members of the sales team couldn't connect with customers due to a compromised cloud account? Every time that spam and malicious email gets blocked, you're preventing downtime from hurting the business. Plus, every time a malicious email gets through, the incident might take time away from help desk professionals and IT administrators.

The average annual cost of phishing-related attacks is now more than **$14.7 million.**[10]

Every knowledge worker loses an average of **seven hours** of productive time each year because of phishing.[11]

The average ransomware attack in 2021 cost its victim **$4.54 million.**[12]

Victims of business email compromise (BEC) have paid out more than **$43 billion** to criminals since between 2016 and 2021.[13]

10 Ponemon Institute. "**2021 Cost of Phishing Study.**" June 2021.
11 Ibid.
12 IBM. "**Cost of a Data Breach Report 2022.**" July 2022.
13 Federal Bureau of Investigation. "**Business Email Compromise: The $43 Billion Scam.**" May 2022.

Monitoring, triage and analysis
Cybersecurity analysts are among the most highly skilled– and highly paid–professionals in the modern IT workforce. And they're in short supply. How security operations teams allocate their time and attention is a matter of strategic importance for your company. Does the solution you are considering make it easier or harder for them to do their jobs? Does it easily integrate into the event monitoring or detection and response solutions that are currently in use in your environment? Maybe you outsource these responsibilities to a service provider. In that case, will the solution enhance your partner's ability to maintain visibility and coverage?

Response and remediation
When your security team is taking action to prevent bad actors from moving across your environment, time is of the essence. Does the solution have a consolidated platform? Can you use policy management to expedite configuration changes? The faster you can block and remediate incoming threats, the less likely they are to progress into damaging breaches.

Automation
Does the solution in question include predefined automation work flows so that it can complete tasks that are part of your regular IT or email security tasks? If your team needs to do a great deal of design and configuration so that the solution can run automated workflows, you should also take that factor into account. If two solutions can both complete the same task, but one takes longer to configure—or requires extensive coding or ongoing administrative overhead—it will cost you more than the other.

Intelligence
Threat hunting is a highly specialised security function that can help you detect vulnerabilities or preventing minor incidents from progressing into breaches. But threat hunting requires skill and expertise that you may or may not have on staff. Does the solution you're considering provide intelligence that will reduce the burden for your team? Does it enable visibility so that they can spend less time and effort on their hunts—or dig deeper with the same number of resources?

Balancing Costs and Benefits in the Real World

Now that we have outlined the costs and benefits that a security solution might bring to your organisation, let's take a closer look at how you calculate the total value of solutions in the real world.

What are the *real* value differences between so-called "free" or "low cost" capabilities and those that you'd get with an industry-leading solution?

When weighing solution options, you can calculate the total value of each solution by subtracting the costs from the benefits. We will use two examples to show you how:

Example 1

Email security

Today's email attacks target people, not systems. They use social engineering tactics to lure users into visiting malicious sites and giving up credentials. An effective email security solution must have the ability to prevent, detect and respond to threats that target your employees. It must also be able to give security teams the visibility and insights they need to be effective – without being hard to configure or administer.

Evaluating costs

Let's assume that you are a financial services firm in the United States with 15,000 employees and you are evaluating two email security solutions, one of which is a so-called "free" solution bundled in with an existing product you licence. This example assumes that a full-time employee (FTE) costs $150,000 per year.

Your costs (over three years) may look something like this:

COST CATEGORY	EMAIL SECURITY SOLUTION A	EMAIL SECURITY SOLUTION B
Licensing costs	-$787,500	-$0 (because you will keep the bundle, the new solution is additive)
Professional services	-$27,000	-$0 (already deployed)
Employee time: deployment	-$6,250 (1 FTE for 0.5 months)	-$0 (already deployed)
Employee time: ongoing	-$450,000 (1 FTE per year)	-$450,000
Total	**-$1,270,750**	**-$450,000**

In this case, an initial glance at the costs might lead you to believe that Solution B seems like a better value, with solution A ringing in at over $700K more than Solution B. The professional services and deployment for the incumbent are prior expences, so we are excluding those values.

Email security solution benefits

To understand the total value of the solutions, however, you must also consider the benefits of each, including risk resistance and workforce efficiency benefits.

Over the course of three years, they may look something like this:

BENEFIT CATEGORY	EMAIL SECURITY SOLUTION A	EMAIL SECURITY SOLUTION B
Risk resistance	$5,707,901	$4,442,698
User productivity	$1,200,208	$974,788
Monitoring, triage and analysis	$1,532,510	$1,224,135
Response and remediation	$2,651,671	$2,153,641
Automation	$0	$756,685
Intelligence	$0	$0
Total	**$11,092,290**	**$9,551,947**

Solution A provides significantly more risk resistance and adds more workforce efficiency benefits, complicating the picture. Solution B has an extra feature, so in this case we would investigate whether we could add that option with solution A, which would increase our ROSI.

Finally, you will want to weigh the total costs against the benefits for each solution to get the total value of each solution:

CATEGORY	EMAIL SECURITY SOLUTION A	EMAIL SECURITY SOLUTION B
Benefits	$11,092,290	$9,551,947
Costs	-$1,270,750	-$450,000
Total value	**$9,821,540**	**$,9,101,947**

Here the full picture emerges. Solution A may come with a higher price tag, but its total value is over $700,000 more than the "free" option of Solution B. The comparison should also be weighed against your business's requirements.

Example 2

Cloud security

Modern cloud application security solutions help organisations manage people-based risks in the cloud. Today's enterprises are making use of cloud platforms and services on an ever-greater scale. They're doing so to enable to enable hybrid and remote workforces as well as to take advantage of the flexibility and business agility that the cloud makes possible. But for all their benefits, cloud-based applications and services also create new risks. A cloud application security broker (CASB) secures IT-approved applications in the cloud. However, it also provides visibility and control over how people access and use apps in the cloud — and how they share sensitive data.

In 2021, the number of breaches that involved cloud resources was greater than the number of breaches involving on-premises assets for the first time ever.[14] As businesses move to the cloud, attackers are following them. As enterprises continue to rely more heavily on software-as-a-service applications such as Microsoft 365 and Google Workspace, we can only expect this trend to continue.

If you are moving a significant portion of your infrastructure to the cloud, it's not really a question of whether you need a cloud security solution, but more a question of which one.

Evaluating costs

Let's assume that you are a healthcare organisation in the United States with 15,000 employees and you are considering a new cloud solution (Solution A) and comparing it with your existing solution (Solution B). This example also assumes that a full-time employee (FTE) costs $150,000 per year.

Here's how your costs may break down over three years:

COST CATEGORY	CLOUD SECURITY SOLUTION A	CLOUD SECURITY SOLUTION B
Licensing costs	-$776,250	-$765,000
Professional services	-$26,000	-$0 (already deployed)
Employee time: deployment	-$6,250 (1 FTE for 0.5 months)	-$0 (already deployed)
Employee time: ongoing	-$450,000 (1 FTE per year)	-$450,000
Total	**-$1,258,500**	**-$1,215,000**

In this case, the costs of Solution A slightly outweigh the costs of Solution B. The professional services and deployment for the incumbent are prior expenses, so we are excluding those values. The real difference between the solutions will come out by comparing the benefits.

IMPORTANT NOTE: If your existing solution is an on-premises identity and access management solution and you are considering moving to a CASB, there may be additional hardware costs to evaluate. Moving to the cloud usually means less spending on hardware, but your overall savings will depend on which cloud vendor you choose.

14 Verizon. "2021 Data Breach Investigations Report." May 2021.

Evaluating benefits

As with your email security evaluation, you must also consider the benefits of each solution to compare the total value of each option. Over the course of three years, they may look something like this:

BENEFIT CATEGORY	CLOUD SECURITY SOLUTION A	CLOUD SECURITY SOLUTION B
Risk resistance	$6,137,377	$3,625,216
User productivity	$42,684	$34,667
Monitoring, triage and analysis	$104,339	$84,742
Response and remediation	$94,853	$77,038
Intelligence	**$1,264,707**	**$1,027,174**
Total	**$7,643,961**	**$4,848,837**

In this case, Solution A provides significantly more risk resistance as well as more workforce efficiency benefits.

	CLOUD SECURITY SOLUTION A	CLOUD SECURITY SOLUTION B
Benefits	**$7,643,961**	**$4,848,837**
Costs	-$1,258,500	-$1,215,000
Total value	$6,385,461	$3,633,837

Due to its increased risk resistance and workforce efficiency benefits, Solution A provides nearly double the value of Solution B.

The Big Picture

Making the decision to invest in a security solution requires you to carefully weigh the costs and benefits that come with each of the available options. It is crucial to find a solution that will meet your short-term budget needs, but it is just as important to find one that will mitigate the financial risks that cyber crime poses to your business over the longer term.

Options with low licensing costs might seem like a good deal at first glance, but you must consider a much broader set of factors if you want to make the best possible decision. Look for a vendor whose solution provides holistic, comprehensive coverage for today's most exploited attack vectors.

Remember that integrations with other security solutions will provide your team with much-needed visibility. Bear in mind that this visibility can provide the intelligence you need to implement controls that reduce risk.

So can workflows that are easy to operate and administer and accurate, high-performing automated threat blocking. In a world where security professionals are in short supply, anything that makes it easier for those on your team to do their jobs will reduce labour costs. At the same time, it will enable them to contribute more value.

Visibility also provides insight into people-based risks that may otherwise slip past your radar. Today's attackers know that people are the easiest way into your organisation. As a result, the most effective solutions are those that are focused on identifying and reducing these risks. Keeping your focus on people-based risks is the best strategy for optimising your security spending.

Take the Next Steps

Proofpoint offers comprehensive, intelligent email and cloud security solutions to protect your people from today's most dangerous threats. To learn more and request a rapid risk assessment for your business case, **visit proofpoint.com**.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations’ greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organisations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0501-012-02-01 09/22