Moving to a More Efficient Cybersecurity Strategy

Corporate security leaders tend to understand that it is not optimal to try to secure every single business or IT asset at the same level. The very essence of risk management is the recognition that perfect protection is nonexistent. Cybersecurity budgets may be growing but they are not unlimited. The challenge is to figure out how to spend efficiently on cybersecurity — a plan that will invariably change every year or so. Threats evolve. Compliance requirements change. Business priorities shift. Security plans and budget allocations must evolve with them. This is “spending smart” on security. This paper examines how cybersecurity leaders can devise effective, optimal security plans that prioritize spending to appropriately balance risk with cost in order to support business objectives.

“He who defends everything defends nothing.”

Frederick the Great

Introduction

Frederick the Great, the 18th Century King of Prussia and one of the most successful military leaders in history, understood well that a meaningful defense had to be focused on protecting that which he valued most. Corporate security leaders can take inspiration from the philosophy of “Old Fritz” as he was known. Trying to secure every single business or IT asset at the same level is neither optimal in security terms or efficient as a matter of budget. There isn’t enough money or time to mitigate every risk. Risks are managed, never totally eliminated. Even when security budgets grow, they are never unlimited.

At the same time, the threat environment grows bigger and more complex with every passing year. The challenge is to make the right tradeoffs to manage your specific business risks given your resources and priorities. You have to figure out how to spend efficiently on cybersecurity. This paper reviews how some traditional approaches to information security are increasingly deficient in today’s environment. It offers insights based on CenturyLink’s extensive security experience in “spending smart” on cybersecurity. This paper examines how security leaders can devise effective, optimal security plans that prioritize spending to appropriately balance risk with cost in order to support business objectives.
Today’s Threat Environment

A quick glance at the headlines over the last few years will tell you that the threat environment today has grown more serious than ever. Malicious actors are brazenly raiding some of the best known, and best-funded organizations in the world. Major retailers, healthcare providers and the US Federal Government have all felt the sting of massive data breaches.

Just as Old Fritz faced off against armies from Russia, Austria, France and Sweden, you might be defending against the cyber warfare units of sovereign powers. You’re probably confronting the simultaneous threats of spear phishing, ransomware and distributed denial of service (DDoS) attacks. Industry data supports the notion that the world is indeed growing more threatening, in cyber terms. PWC reports, for example, that security incidents grew by 38% from 2014 to 2015. The trend appears to be on the upswing in 2016.

The Challenge of Securing a Blurred Perimeter

Old Fritz actually had it easier than today’s CISOs in one important regard. He knew where his lines were. In his day, if you had horses and cannons lined up, that was your perimeter. The enemy would have to fight to get through. Until about a decade ago, most InfoSec models worked on this kind of perimeter-based model. The firewall and the corporate network defined the boundaries of your enterprise. What was in was in. What was in the “DMZ” was in the “DMZ,” and so forth. This is no longer the case in any meaningful way.

InfoSec today is dominated by a blurred perimeter. Your business and IT assets are distributed across multiple on-premises, colo, private cloud and public cloud environments. Your organization may be sharing data with external third parties, to whom you provide programmatic access through standards-based application programming interfaces (APIs). Where your organization ends and the outside world begins is not so easy to see any more. The frenzied pace of mergers and acquisitions (M&A) accelerates the uncertainty of the perimeter. Figure 1 captures the overlapping risk factors that contribute to today’s blurred security perimeter.

Newer technologies, such as mobile, wireless and the Internet of Things (IoT) further blurs the perimeter. For example, the user of a mobile app developed by one of your partners might be accessing your back end systems through an API. Do you have any idea what kind of security features his or her mobile device has? Is your data encrypted on that device?

The people who work for you also make today’s perimeter harder to see and enforce. If your organization is like most, you probably have full time employees, contractors, outsourcing firms and maybe even offshore people accessing your core IT assets. Or worse, an unknown contractor for a partner firm might have privileged access to your systems.
The Deficiency of Traditional Security Approaches

The growing threat environment creates a negative synergy with the blurring perimeter to exert more pressure on your security budget. It’s tempting to create a Security Operations Center (SOC) to stay on top of all threats, but this is feasible only for the largest organizations. And, even if you could, would it be the best use of your budget? Today, every countermeasure and control should be assessed for its utility and necessity in this way.

Hardware and software alone are not sufficient for security in today’s world. We find one common problem to be over-defending in one area while exposing themselves to other vulnerabilities. For instance, an organization might focus its time and budget on a specific type of countermeasure like Data Loss Prevention (DLP) or packet capture while not taking care of basics. Consider the fact that many of the most serious attacks exploit known vulnerabilities.¹ Patching is basic. It works, too. According to CERT, 85% of targeted attacks that exploit unpatched vulnerabilities are preventable. But, by diluting focus and budget dollars, it’s possible to miss doing the basics right.

A lack of personnel is also to blame for gaps in security. For some organizations, it’s a big challenge just to find people who know how to take care of security. According to Frost & Sullivan, the tech world will face a deficit of nearly 1.5 million security personnel by 2020.² Not having enough people compounds the problem of diluted budget and focus in security.

Allocating Security Planning and Funds According to the Heat Map

Given that you can’t, as Old Fritz warned, defend everywhere, where should you allocate your security resources? One proven practice is to conduct a Business Impact Analysis (BIA) and identify risks that carry the greatest potential business loss. Then, focus on those. After all, not all risks are alike in terms of business impact. For instance, a hack of a company website might prove embarrassing, but it can be fixed relatively quickly and cheaply. Conversely, a breach of a customer database can be extremely expensive to remediate. There can also be long term reputation damage that may never be fully repaired.

Business Impact Analysis

A BIA usually involves assessing each risk and assigning it a score based on its likelihood and business impact. For example, as shown in Table 1, the likelihood, impact on IT and impact on the business are ranked on a score of 1-10. The higher the number, the greater the likelihood or impact. In this example, an email server outage is highly likely, so it gets a score of 6. However, the impact of an email server outage on IT and the business scores 2 and 1, respectively. An email outage is a hassle, but it won’t wreck the business. It gets a total impact score of 9. On the other hand, a database breach, which is unlikely, has a very severe impact on IT and the business. It scores 22 total.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Likelihood Score</th>
<th>Impact on IT</th>
<th>Impact on Business</th>
<th>Total Impact Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email server outage</td>
<td>6</td>
<td>2</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>Website hack</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Database breach</td>
<td>1</td>
<td>10</td>
<td>10</td>
<td>22</td>
</tr>
<tr>
<td>ERP hacked</td>
<td>1</td>
<td>8</td>
<td>5</td>
<td>14</td>
</tr>
</tbody>
</table>

Table 1 – The Business Impact Analysis (BIA) scoring chart.
Security Managers can then plot their risk scores on a chart like the one shown in Figure 2. This is sometimes called a “Risk Heat Map.” The higher the likelihood and business impact, the “hotter” the risk. The hotter the risk, the more security resources it deserves. Budget allocation should follow the heat map. The hottest risks get the most money. In some cases, the organization may want to supplement security countermeasures with insurance or other controls that mitigate the potential business impact of a risk. As an alternative to insurance, it may be preferable to outsource a workflow rather than carry the full risk.

**Updating the Heat Map for Today’s Risk Environment**

The new blurred perimeter affects the heat map exercise. New risk factors such as third party entities with API access should be considered in estimating the likelihood and impact of a security incident. Rethinking the BIA along these lines leads to the updated BIA chart shown below. The new chart in Table 2 includes columns for the number of external entities involved in a solution at risk as well as the architectural complexity of that solution. These added factors will affect the likelihood and impact scores. A complex solution with many external entities involved is going to have a much greater impact if it is breached than a simple solution with few entities. If you don’t account for new risk factors, you may allocate to areas that are “colder” than you realize and missing those that are truly “hot” and full of risk.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Number of external entities involved in the solution</th>
<th>NEW Likelihood Score</th>
<th>Complexity of architecture</th>
<th>NEW Impact on IT</th>
<th>NEW Impact on Business</th>
<th>NEW Total Impact Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Hosted) Email server outage</td>
<td>Low</td>
<td>Low</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Website hack</td>
<td>Low</td>
<td>Low</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Database breach</td>
<td>High</td>
<td>High</td>
<td>10</td>
<td>10</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td>ERP hacked</td>
<td>High</td>
<td>High</td>
<td>8</td>
<td>8</td>
<td>21</td>
<td></td>
</tr>
</tbody>
</table>

The updated BIA chart shows a change in “heat” for several of the risks. Now, the ERP system is integrated with multiple external entities. It is highly complex. If it is breached, the impact score will now be 21, rather than 14. In contrast, by switching to hosted email, the likelihood of an outage is lower. The impact of the outage on IT and the business is lower as a result. The management of the risk — and any potential incidents, has been shifted to the email hosting provider.

Using the new heat map approach enables you to be more accurate in your allocation of security resources. In this example, it would now be wise to put more security resources into protecting the ERP system than the earlier analysis might have suggested. And, email outages require less funding to mitigate. The result should be a more effective overall level of security due to efficient security budgeting.
The CenturyLink Approach

CenturyLink can be your partner for developing a more efficient security strategy. If you accept that you do not likely have the time, personnel, tools or resources to mitigate all of your high-impact risks, consider how we can help. Our security services, honed over years working with some of the world’s largest enterprises, are designed to give you capabilities that would be difficult to create in-house.

We provide a unified system of security services that covers the entire IT stack. With this approach, we are able to reduce security and instability risks that arise from managing and integrating disparate technologies, services and SLAs across multiple vendors. It’s a true ecosystem of security services that ranges from DDoS attack mitigation, to monitoring and management of basic protective devices like firewalls, to handling the entire lifecycle of an attack. Our approach incorporates macro threat intelligence, advanced analytics and SIEM technologies along with proactive detection, containment and incident response services.

CenturyLink is known for expert security consulting by specialized security and SOC pros. Our expertise goes into securing our millions of customers, 550k fiber route miles of global network and billions of dollars in business assets. We can evaluate your regulatory environment and suggest the tailored delivery of standard solutions. These can be easily added to CenturyLink hosting, cloud, network and colocation services.

Services can be fully managed, co-managed or self-managed. They are available on-premises and/or hosted. Our dashboards allow you to visualize your security posture, gain insight into threat patterns as well as speed decision making and incident resolution. CenturyLink security clients get 24/7 continuous monitoring and incident response from our commercial SOCs, which are staffed by over 250 researchers, testers and GIAC Certified Intrusion Analysts.

Conclusion

Old Fritz knew when to call in reinforcements if battle conditions warranted it. You might want to consider this option, too. The reality of today’s security environment is that you need to be good at appropriately managing the risks you face using the budget and resources at your disposal. You can be efficient with your security budget while achieving a higher level of risk mitigation. To accomplish this goal, you have to first understand your particular risk “heat map,” especially as it may have changed in recent years with new complexities and interdependencies.

Then, assessing what you can do best in-house, it is possible to work with a partner like CenturyLink to provide the security advising and services needed to fill the gaps and help strengthen your security posture. Let CenturyLink join your security team to make your organization more secure while you improve the efficiency of your overall security budget.
About CenturyLink Business

CenturyLink, Inc. is the third largest telecommunications company in the United States. Headquartered in Monroe, LA, CenturyLink is an S&P 500 company and is included among the Fortune 500 list of America’s largest corporations. CenturyLink Business delivers innovative private and public networking and managed services for global businesses on virtual, dedicated and colocation platforms. It is a global leader in data and voice networks, cloud infrastructure and hosted IT solutions for enterprise business customers.

For more information visit www.centurylink.com/enterprise.


Global Headquarters
Monroe, LA
(800) 784-2105

EMEA Headquarters
United Kingdom
+44 (0)118 322 6000

Asia Pacific Headquarters
Singapore
+65 6768 8098

Canada Headquarters
Toronto, ON
1-877-387-3764