QUANTIFY AND COMMUNICATE: THE ROI OF CYBER SECURITY

Whitepaper F-Secure
INTRO

As a cyber security professional, you know that a comprehensive defense is essential for a modern business. But we know that budgets are tight and you are under increasing pressure to justify security spending to other stakeholders that are not as clued up on the current threat landscape as you are.

Things are moving in the right direction though, our latest CISO survey found that 78% of CISOs believe that board priorities and attitudes towards cyber security have positively improved. However, only 10% believe that board priorities and attitudes have changed at the highest level (scoring 9 or 10), leaving much more work to be undertaken.

This whitepaper will outline the logic behind the ROI calculator that F-Secure has developed to help you quantify and communicate the value of implementing cyber security solutions to your CFO/CEO. It will explain the chosen methodology and risk scenarios so that you can be better prepared to defend your ROI estimate to them. We will also look at a couple of worked examples of ROI calculations for our own cyber security solutions.

Finally, we’ll give you the option to book a session with one of our experts to walk you through calculating your own ROI estimate and help you prepare your business case for an investment in F-Secure Elements.

F-Secure Elements is our all-in-one security platform that includes endpoint protection, endpoint detection and response, vulnerability management and Microsoft Office 365 protection.
ROI AND THE CURRENT THREAT LANDSCAPE

The simplest way to think about the return on a cybersecurity investment is in terms of the potential losses that it helps you avoid or mitigate. This will resonate with other stakeholders as well. According to the CISO survey 79% of CISOs and their CEOs see cyber security predominantly as a risk mitigation or compliance practice.

Board discussions about cyber security will start with questions about the current threat landscape. The threat landscape is constantly evolving so in order to present the most up to date information you can check our monthly threat updates published on our website.

The key themes and backdrop that these updates should be presented against is that we live in a digital age where we spend more time online than we do asleep, meaning we are constantly at risk. Businesses today face the same threats as nation states, with a fraction of the resources available for defense.

Cyber crime is projected to cost $8 trillion per year by 2025. It represents the greatest transfer of wealth in history.
THE F-SECURE MODEL

Quantifying the cost of a security breach is difficult. Direct costs like damages to equipment or increased insurance premiums are easy enough to calculate, but the wider impact of business disruption and reputational damage are less concrete.

Our own model calculates risk probability using a combination of publicly available data and F-Secure’s own proprietary database.

It takes seven different risk scenarios into account:

<table>
<thead>
<tr>
<th></th>
<th>Unauthorized access via the supply chain</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(e.g. business disruption caused by a supply failure, need to replace a supplier)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Compliance failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>(e.g. legal challenge, additional audit costs, fines)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Critical vulnerability in software component</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>(e.g. patching or remediating newly discovered vulnerabilities, disruption caused by business practice changes, software replacement)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Malware outbreak</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>(e.g. business disruption, incident response and forensic costs)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Business disruption caused by ransomware</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>(e.g. business disruption, incident response and forensic costs)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>System intrusion - intellectual property theft</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>(e.g. reduced growth, damaged investor relations)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Information breach - personal information</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>(e.g. incident response and forensic costs, regulatory fines, class actions).</td>
</tr>
</tbody>
</table>
Of course, risk scenarios outside of these seven exist, and our model does not account for them. However, we believe that these seven constitute the most common scenarios that most organizations face.

To quantify these risk scenarios, we use a four-stage methodology that is based on the FAIR Institute’s Factor Analysis of Information Risk. Stage one is identifying the components of the scenarios above, what is at risk and who is likely to be attacking it.

Stage two is working out how often a loss is likely to happen. Because perfect data on cyber security incidents doesn’t exist, we take the data we have and work out the rate of occurrence based on that. Then when new data becomes available, we can adjust the probability.

Stage three is working out the magnitude of losses. Using this model, we can estimate where the cost of 90% of attacks against an organization like yours will fall (of course this means that 5% of attacks will be more or less costly). The model also lets us estimate the probability of a risk arising in the next 12 months.

Stage four is quantifying this risk in €€€. This is where we simulate losses for all seven scenarios with and without your chosen solutions implemented and use those numbers to calculate a return on investment figure.
Example calculations

To demonstrate how these estimates might look we have taken two example calculations based on hypothetical companies. The first is a medium-sized German clinic chain and the second is a small b2b software developer based in the UK.

The below calculations show their estimated risk reduction and ROI using their chosen F-Secure solution.

If you decide to use our calculator, our experts will walk you through the process in further detail. They will help you clearly demonstrate the link between your company specific data, chosen solutions and the risk summary you receive.

The examples below were calculated for the F-Secure Countercept solution, using financial data from listed comparables.
COMMUNICATING ROI TO THE BOARD

To be accepted by a CFO, you will need to demonstrate that the ROI calculation uses reliable figures for the company-specific inputs. For example, the loss estimates take into account the largest value of invoice that is regularly paid by your company. Your finance department should be able to supply you with this information or at least provide a credible estimate.

You will also need to be able to explain the reasons for choosing the methodology and its limitations.

Our model has been built using the most widely accepted risk estimating methodologies within the industry. It is based on the same risk analysis framework as those used to model other complex scenarios with a high number of inputs and uncertain input data, such as those used to simulate risks in insurance, medicine, and power plants.

However, we don’t have access to the same wealth of data that an insurance company does, and you may face questions from the board about sample size and the level of confidence they should have in the model as a result. It is worth reminding them that balance has to be struck between the level of confidence one can have in the results and the need to make a timely decision.

Data gathering is costly and slow if it is possible at all. We use customer data that is easy to gather and industry data from F-Secure and other high-quality sources to produce logically-derived, defensible loss estimates and a clearly stated confidence level.

The point of the model is not to predict anything, but to make estimates about the amount of losses that are likely to be mitigated over a period of time with our solutions. This allows you to make a business case for implementing the solution that is clearly quantified and based on the available data.

It is also worth noting that taking no action has additional costs beyond the estimated losses in our risk scenarios. An Exabeam study found that the typical organization wastes 286-424 hours of IT professionals’ time on false positives every week. If automation technology in your chosen solution can provide an initial filter that eliminates even half of these, it will be a huge time saver. It also frees up employees to work on other initiatives that could improve security posture.

An investment in a security solution is both an insurance policy against being attacked and a long-term investment in the resilience and productivity of your business in the modern world.
**MAXIMIZING YOUR ROI**

At its most basic, maximizing ROI means minimizing the costs of your cyber security without compromising your threat mitigation ratio. In this section we’ll focus on factors to consider when choosing a solution to make your investment as efficient as possible.

**F-Secure Elements** is our all-in-one security platform that includes endpoint protection, endpoint detection and response, vulnerability management and Microsoft Office 365 protection.

F-Secure Elements has been designed with all of these ROI concepts firmly in mind, but they are important when considering an investment in any cyber security solution.

**Usage-Based Security**

Make sure that you only pay for what you’re using. Usage-based models let you pay for the number of endpoints that are signed up to for each solution. When the business environment is uncertain, minimizing fixed costs is financially prudent. But it could also help you maximize your ROI.

If you know for certain how many endpoints and what solutions your business will need, then a long-term license may prove to be more cost effective from an ROI optimization perspective. However, in our experience many companies on this kind of contract have ended up paying for services they could not use, particularly during the pandemic.

**Security as a Service**

Buying cyber security as a service through a managed service partner is likely to be the most efficient option for SMEs in terms of maximizing your ROI. This is because it saves on workforce costs like monitoring and taking care of security updates.

Cyber security experts are difficult and expensive to hire and need constant training to keep up to date with the current threat landscape. These costs can be minimized by using a security partner.
**Remove waste from your tech stack**
Many companies have responded to the ever-developing threat landscape by employing a complex array of specialized solutions from various vendors. Each individual solution will require its own management and it’s easy to lose track of.

Good cyber security starts with good visibility. At F-Secure we believe that the future of cyber security is all-in-one solutions that allow multiple products and services to be monitored and managed from a single console. This allows you to see exactly what you’re using and make sure its always optimized for your current security needs.

**Choose an integrated solution**
If you have siloed solutions from different vendors, or even the same vendor, they will likely lack the ability to automatically share data. If a threat is detected by one system, it requires an administrator to ensure configuration changes are carried out on the other solutions.

With modern integrated solutions all the constituent parts are designed to work together, and actually work better, the more you add. This is because they automatically share data and when a response is triggered in one it will be executed across all.

This increases your ROI because it optimizes spending on time and resources. If you’re using siloed solutions you likely have a different person or team responsible for each one. Whether or not you’re outsourcing, you want to make sure that time and resources of the human element of your solution is optimized.

**Choose a cloud-native solution**
Cloud-native management means you don’t need to invest in management server hardware, software, or maintenance.

With cloud-native solutions, all endpoint software and security updates are handled automatically, helping you maintain the highest possible level of protection at all times and reducing update-related costs.
WANT TO KNOW MORE?

Get in touch with our team today so that we can take your business-specific information and deliver ROI estimates to support your business case for Elements.

Request a consultation

ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We’re closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry’s best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world’s most potent threats.

Together with our network of the top channel partners and over 200 service providers, we’re on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com/business | twitter.com/fsecure | linkedin.com/f-secure