Modelling Cyber Security Risk Across the Organization Hierarchy

Security issues have different causes and effects at different layers within the organization – one size most definitely does not fit all. Likewise, the investment in security controls needs to take into account the level of risk and return on investment to reduce the risk to an acceptable level – throughout the organization. Are you finding the black swan or the elephant in the room?

By applying the *Bow Tie* model, we can determine the threats, vulnerabilities and required controls for cyber-security:

- we can model a hierarchy of causal relationships that could lead to an incident and controls that could reduce the likelihood of the incident occurring (fault tree); and
- given that an event has occurred, we can model the potential consequences and contingent controls (event tree).

We will use a targeted 'phishing attack' as an example of the necessary controls through the layers of the organization and phases of response.

The explanations for the causes and likelihood of Event Scenarios can be determined for the various organizational cyber security layers. Note that multiple threat events and control failures may lead to multiple Event Scenarios which in turn may culminate into a catastrophic event. *Refer to the Fault Tree section.*

The consequences from the Event Scenarios and the efforts to mitigate and to return to normal operations from the results of the Event Scenarios are modelled in the Event Tree. Note that the consequences may be different for the various organization layers and types of Event Scenarios. *Refer to the Event Tree section.*
# Organizational Cyber Security Layers

The causes and effects of event scenarios depend on where and at what level of the organization we wish to assess. Furthermore, a successful compromise at one level can contaminate the layers above and below this layer.

Here is a review of the various layers of security.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>14 Regulatory</strong></td>
<td>Legal restrictions promulgated by governments</td>
</tr>
<tr>
<td><strong>13 Policy</strong></td>
<td>Principles of behaviours adopted by the organization</td>
</tr>
<tr>
<td><strong>12 Standards &amp; Guidelines</strong></td>
<td>Instructions and yardsticks for measure and control</td>
</tr>
<tr>
<td><strong>11 Process</strong></td>
<td>A systematic series of procedures directed to some organizational deliverable</td>
</tr>
<tr>
<td><strong>10 Procedure</strong></td>
<td>A documented set of activities as called for in a process</td>
</tr>
<tr>
<td><strong>9 Activity</strong></td>
<td>The smallest unit of work or behaviour called for in a procedure</td>
</tr>
<tr>
<td><strong>8 People</strong></td>
<td>You &amp; I</td>
</tr>
<tr>
<td><strong>OSI layers 1 to 7</strong></td>
<td>Open Systems Interconnection Reference Model, or simply the OSI model. Network attacks have moved up the OSI network model over time, climbing from network attacks in the 1990s to session attacks and application layer attacks today.</td>
</tr>
</tbody>
</table>

![Diagram showing the OSI layers with Application, Presentation, Session, Transport, Network, Data Link, and Physical layers, indicating increasing difficulty of attack detection from Physical to Application layers.](image.png)
Layers of Protection – Swiss Cheese Model

For an event to occur, the various possible causes need to occur. This is called the Swiss Cheese model, where layers of the system controls cause defence-in-depth. For an attack to be successful, each layer in the cheese needs to have a hole (vulnerability) aligned with the adjacent layer. Each layer in the organization has a role toward prevention, detection, mitigation or recovery from the event. Providing the controls complement each other across the organizational layers (the holes in the Swiss Cheese are blocked by the other control layers) a threat agent will be blocked from causing a hazardous event. However, should a layer of control fail (the holes in the Swiss Cheese line up), an incident will likely occur.

E-mail Phishing Example of Controls by Security Layer

A phishing attack can only be successful if the layers of technological and procedural controls are missing or have failed. Phishing attacks represent a combination of user and technological failures. Before the user is ever confronted with a phishing e-mail, there are opportunities to block the attack at the network components and at the mail server.

Fault Tree Analysis

This is a technique which starts with the undesired event (top event) and determines all the ways in which it could occur. These are displayed graphically in a logical tree diagram. Once the fault tree has been developed, consideration should be given to ways of reducing or eliminating potential causes / sources. Fault Trees are composed from events with relationships that connect the events together reflecting the structure and relationships within the organization and to the organization environment.

We will take the e-mail phishing scenario to build a simplified fault tree model.
Illustration 3: Fault Tree analysis across the cyber security layers
<table>
<thead>
<tr>
<th>Security Layer</th>
<th>Threat Event</th>
<th>Possible Countermeasure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layers 2, 3, 4</td>
<td>Malicious e-mail arrives from some internet source over service provider network.</td>
<td>Technologies for detecting and deleting phishing emails can be implemented in the internet infrastructure to block these attacks before they reach mail servers.</td>
</tr>
<tr>
<td>Layers 6, 7</td>
<td>Malicious e-mail has arrived at the server, most likely from an un-trusted source but may have arrived from an outside trusted source that had been infected with the e-mail payload.</td>
<td>At the mail server there is another opportunity to implement technologies to quarantine phishing emails.</td>
</tr>
<tr>
<td>Layer 8, people</td>
<td>E-mail recipient unwittingly opens e-mail that should have been suspicious, allowing address book of the user account to forward the malicious e-mails to other accounts. Recipient also convinced to open attachment, which unleashes payload application.</td>
<td>It is only if these first 7 OSI layers have failed to block a phishing attack that a user becomes involved. If users have been properly trained to recognize and report phishing attacks, these attacks can be blocked at this stage. User awareness programmes should be designed to ensure that users are able to recognize a potential phishing attack and know where to report it. Users may still be spoofed by social engineering methods that make use of a well-crafted phishing email.</td>
</tr>
<tr>
<td>Layer 9, Activity and Layer 10, Procedures</td>
<td>Payload of opened e-mail is propagated along with automatically forwarded packets across e-mail accounts via e-mail services.</td>
<td>Even if a user clicks on a malicious link in a phishing email, all is not lost because technologies exist to warn users of potentially harmful links and quarantine the attachments. The user has the opportunity to report attempted phishing attacks to enable administrators to delete any associate unopened phishing emails on the mail server.</td>
</tr>
<tr>
<td>Layer 11, Process</td>
<td>E-mail payload executes across connected networks, causing malicious activity to propagate across the network, bypassing normal network controls.</td>
<td>But if a user decides to open an email even though it has been quarantined, the email client should still be able to prevent malicious code from executing. The network can be equipped to be a layer of defense and should be able to detect and block malicious activity, identify rogue clients and prevent any infection from spreading. Interrupting the criminal’s discovery process as quickly as possible is the ideal response, and requires the organization to allocate the budget, resources and necessary skills.</td>
</tr>
<tr>
<td>Layers 12 and 13, Policy, Standards and Guidelines</td>
<td>Contingency plans are not followed or are proven to be ineffective. Network administration either fails to respond properly or panics.</td>
<td>Once the security basics are in place, organizations need to focus on reducing impact and understanding how to recover more quickly. Organizations need to understand what has happened and must be absolutely clear about how they respond to an attack.</td>
</tr>
<tr>
<td>Layer 14, Regulatory</td>
<td>Interconnected organizations receive the malicious traffic without warning. Adequate response is not possible because they were not notified in a timely manner, metrics are not kept, heuristics were not assessed.</td>
<td>Organizations need to have a clearly-defined process in place for notifying and reporting unexpected incidents. Collaboration between organizations within and across sectors is getting better, and is encouraged by the government security initiatives in many countries.</td>
</tr>
</tbody>
</table>
Event Tree Analysis

Consequence analysis determines the nature and type of impact which could occur assuming that a particular event situation or circumstance has occurred. An event may have a range of impacts of different magnitudes, and affect a range of different objectives and different stakeholders. When we have established the context of the event we can decide what types of consequence to be analyzed and which stakeholders would be affected.

From the preceding Fault Tree Analysis example, we can choose threat events to create the event tree model. As an illustration, we will pick as an initiating event the acceptance of the malicious software at the e-mail server. We assume the event has already happened: somehow malicious e-mail data, of unknown threat level, has passed through the network layer control.

The combination of fault tree and event tree analysis can quickly get complicated. We should start with a high level analysis and work in the detail over time. This is where an automated method can help us keep track of the complexity and the numerous inter-relationships of cause and effect.
Measure of Effectiveness

From a review of remediation methods for targeted phishing scenarios, no single solution is fool-proof. Even for the expensive solution – R4 in this case – we need defence-in-depth.

Management can then select an optimal and acceptable method to control the risks by:

- comparing the potential impacts determined from the fault tree analysis
- to the cost of selected remediation methods from the event tree that would reduce the risks to an acceptable level.

Because of the costs and skills required to administer and manage the more complex applications, management may have to accept the risks of implementing a cheaper and less effective remediation solution.
Bayesian Networks for Modelling Risk

This process of fault tree analysis, event tree analysis, and control selection can be modelled using Bayesian Networks\(^1\) for the following benefits:

- Explicitly models causal factors including incorporation of expert judgment in scenarios of insufficient data and accommodate causal explanations;
- Reason from effect to cause and vice versa. The probability distributions for every unknown variable will be updated whenever an observation is entered into any node.
- Reduces the burden of parameter acquisition. The process is modular and compact making the elicitation of probabilities easier and explaining the model results easier.
- Overturns previous beliefs in the light of new evidence. The model is flexible.
- Makes predictions with incomplete data. There is no need to enter observations about all inputs. The model produces revised probability distributions for all the the unknown variables when any new observations are entered. If no observation is entered then the model simply assumes the prior distribution.
- Combines diverse types of evidence including both subjective beliefs and objective data. A Bayesian Network is agnostic about the type of data in any variable and about the way the probability tables are defined.
- Arrives at decisions based on visible, audit-able reasoning. There are no hidden variables and the inference mechanism is based on Bayes theorem.

Conclusion

We have demonstrated how cyber-security risk can be analyzed across the various control layers of an organization. We walked through a malicious e-mail scenario to determine threats, vulnerabilities, and remediation controls.

We used a simplified fault tree model to determine events and relationships that cause security events. We used an event tree for malicious e-mail arriving at e-mail server scenario to evaluate selected remediation controls. We demonstrated how management can make informed decisions toward loss prevention and loss reduction by analyzing the various remediation solutions in terms of cost, effectiveness, and remaining risks. We recommended using Bayesian Networks for modelling the scenarios.

One remediation method we did not mention in the event tree scenario is outsourcing much of the detection and remediation controls. Outsourcing may not reduce responsibility and accountability of your staff, but it may be a good cost effective addition to gain the support of robust remediation tools managed by skilled resources.

We can help.

---