Scenarios for FAIR Analysis

Description:

A cloud-based software company wants a risk analysis. They are most concerned with a data breach. Their product manages client data including network management and vulnerability data. They employ industry best practices. Their target client base includes government agencies, defense contractors and mid-size businesses.

Available data for use in the analysis:

Web-facing server operating systems are Microsoft and so can be a target for attack. Vendor provides frequent updates and patches. Web-facing server interface utilizes popular components and so can be a target for attack. Vendor provides frequent updates and patches. Typical perimeter security is provided including firewalls, intrusion detection systems, application firewalls and proxies, and more. Two factor authentication is available for clients. Once authenticated clients have access to their application suite and data which is on a shared infrastructure with best practices in place for security.

Microsoft recently put out statistics of 8 nation states targeting critical sectors in the last 12 months (8 attacks in 12 months is 8/12=66% likely in the next 12 months at the current frequency rate).

Operations reported that they experience a mix of attack methods such as SQL injection and cross-site scripting on average 15-40 times per day (average 30 days per month we have a range of 450 to 1,350 per month and 5,400 to 16,200 per year). We will estimate threat event frequency directly.

We will estimate vulnerability as derived. You estimate threat capability between 75%-90%. You review the organization's vulnerability data and determine that 2% of web-facing assets ever have a vulnerability unpatched longer than 48 hours from patch release. Internally you find that 5% of assets have configuration or patch vulnerabilities that are un-remediated for up to 12 days. You estimate resistant strength at 95%-98%.

Based on discussions with operations to determine response costs you estimate a typical incident would take 3-5 days at 3x$75 man-hours and 10/hrs per day (3X10X$225=$6,750 to 11,250). You note this is on the conservative side and only includes the initial response, not forensic or full remediations. This is just enough to verify breach, determine means and extent.

You estimate productivity loss as 2.5 hrs per employee per day of response as systems may need to be taken offline, so with 30 employees and pay rates between $45-$90 that range is (2.5x3x30x45=$10,125 and 2.5x5x30x90=$33,750)

Secondary response loss estimate includes initial contact and response to client inquiry only. You estimate between 1 to 3 hours per client for initial contact which would include emails and some phone calls with 1-3 staffers involved all at a salary rate of $55/hr. (1x1x$55=$55 and 3x3x$55=$495)