PIVOTPOINT
RISK ANALYTICS

QUANTIFYING CYBER RISK:
A Success Story in Municipal Government

The City of San Diego has personally identifiable data of its residents, which, if compromised due to a security breach, could force the City to pay for credit monitoring for those individuals affected by the breach. And while its 911 emergency system isn't a revenue-generating asset, it is an essential service delivered by the City and a loss of service could pose liability issues, not to mention reputation and trust issues among City residents.

THE BUSINESS CHALLENGE

Chief Information Security Officers typically struggle to assign a dollar value to potential hacks and make clear the benefits of strong, preventative security measures—particularly if a company hasn't faced a major attack. Presenting the Board of Directors or a government executive with a detailed analysis of average potential losses, severe potential losses, and total exposure can shed light on how to better handle their cyber risk. For example, whether the City needs more cyber insurance coverage and where to bolster its defenses. Board level directors and members of the C-suite want to know:

- How much would a security breach cost us?
- Do we have enough cyber insurance to cover our risk exposure?
- How much risk in financial terms is being reduced if additional security projects are funded?

These questions are critical. If you understand the cost of a breach or the amount of risk you're able to reduce by implementing a security solution, you can strategically prioritize the design and management of your security program.

> *"I have city council...they're asking us, how much is a breach going to cost us? Unless you've had a breach, you have no idea. And you really don't want one of those."*
>
> **– Gary Hayslip, Chief Information Security Officer, The City of San Diego**

CRITICAL SUCCESS FACTORS

To find answers for these questions the City of San Diego searched for strategic tools that could be used to quantify, in monetary terms, the cost of a breach and an organization's risk exposure. The City decided to search for a more thorough security platform that would allow them to test the maturity level of an entire cyber security suite in a "scenario"-based fashion, not just specific components. Critical success factors included:

- Risk presented in financial terms;
- Recommended prioritized mitigations to buy-down risk;
- Compliance with accepted security frameworks (e.g., NIST CSF);
- Threat simulations that model realistic attacks for our industry.

THE SOLUTION

The City of San Diego engaged PivotPoint Risk Analytics and its CyVaR™ solution to analyze the risk of five critical business applications that not only generate revenue for the City, but also are key to protecting its citizens. CyVaR used the business application valuation inputs provided by the City, the defensive posture of the supporting infrastructure, and ran a simulation with realistic threat models, a critical component of the CyVaR product, to calculate the Value-at-Risk for the five applications.

The City found that CyVaR was able to recommend specific actions to reduce risk exposure based on security frameworks, such as the CIS CSC framework (formerly the SANS Top 20), NIST CSF, and ISO270001/2. The recommended actions include monetary risk reduction values i.e., we could lower are total exposure by this dollar value if we implemented a given recommendation. The City also found that once they entered their business applications of interest, their associated value (e.g., revenue contribution, asset value, data liability value, etc.), and the defensive posture of the supporting networks (in this particular case, evaluation against the CIS CSC, they were given not only the "Cost of a Breach", but also insights into the "Full Risk Exposure of the Breach".

> *"You don't want to have this boogie man discussion where you go out and scare everybody. They want to understand: If something bad happens, what's it going to cost us? How bad is it going to get? Without understanding risk it is very hard to answer those questions"*
>
> **– Gary Hayslip, Chief Information Security Officer, The City of San Diego**

THE RESULTS

The CyVaR engine produced the numbers using techniques and algorithms matured by the financial industry. The risk management and financial management staff found the outputs very enlightening. In fact during budget discussions City leadership informed the Department of IT that the data provided from the CyVaR solution was key in providing insight into why the Department required funding for key security projects that aligned with recommended actions generated by CyVaR.

As a result of this engagement, the City is now moving this tool into production to be used by their IT Governance staff and Cyber Security team to better understand the cost of risk for their entire enterprise application portfolio. CyVaR will be used to analyze the value of implementing future technology projects in the City's pipeline prior to actually allocating budget. This visibility into the risk of its application portfolio and future projects is now considered a strategic tool for the Department of IT.