How to Budget for Managed Detection and Response (MDR):

a 6-Step Guide for IT Security

As a security leader, you inevitably balance security needs with budget realities. Your budget makes it difficult to attract and retain qualified security professionals.

At the same time, the volume of security alerts coming off your security products will be overwhelming without a talented team you trust. One way to solve this problem is to hire an MDR provider to monitor your network, detect and investigate intrusions, and assist with rapid response to minimize actual loss or disruption.

Convincing your organization to invest in MDR can take some planning. As you prepare to talk to the C-Suite, you should anticipate the need to educate them on the overall value proposition to the business. You should also be ready to develop a common vernacular so they can understand how and why MDR can produce cost savings through lower costs and reduced business risk.

With those preparatory tasks in mind, here are six tried and true steps to help kick off the budget conversation, create a value proposition, sell MDR based on good business sense, and work toward a budget goal.

- Conduct a Risk Assessment
- Or Get Creative
- Lower Dwell Time to Lower the Impact
- Communicate Full Scope of Potential Impact

info@ci.security
+1 206 687 9100
https://ci.security

CI Security™

- Highlight Opportunities for Cost Avoidance
- Plan for a 1-Year Landing Strip

1. Conduct a Risk Assessment

For many organizations, the first step is to hire security experts to perform a thorough risk assessment[1] . When our consultants perform an assessment, they evaluate your organization's security posture to discover gaps that could lead to breaches and financial losses. For each missing or inadequate control[2] , there's a chance that attackers will exploit it, potentially resulting in a negative financial outcome. To help quantify those outcomes, consulting teams will put together reports on the following financial metrics:

- the true dollar-value impact when a disruption occurs to business processes
- the estimated amount of theft that could occur through fraud or extortion
- the value of your protected records in terms of cost to comply with breach reporting statutes

The assessment facilitates highlighting the specific areas in the security program that require mission-critical funding. This process can also help identify areas that can be de-prioritized, which can pave the way to free up funding for the new line items. When paired with the fact that cyber threats are now considered foreseeable events, you can make the case for MDR by illustrating real security gaps.

2. Or Get Creative

If you cannot budget for a full risk assessment (which can be expensive), you have alternatives.

For example, you may have a certain budget limit for signing authority to hire consultants for small engagements. That provides an opportunity to still leverage the psychology of leadership—it's only believable if a consultant says it in a report. An inexpensive assessment against a standard of practice or regulatory standard will very likely support your assertion that security improvements are needed. This is NOT a risk assessment, and it does not address the likelihood of an event or

its impact. What it WILL show are control deficiencies, such as the monitoring and response process. Such a report from an objective consulting firm can be a powerful ally, and it's possible to get such an assessment for less than $10,000.

If that's still a bit much to budget, self-assess. There are many self-assessment methodologies available to compare against various standards. One example is the payment card industry data security standard self-assessment questionnaire, the PCI-DSS SAQ[3] .

3. Lower Dwell Time to Lower the Impact

Having done your risk assessment correctly, you know that each area of risk is assigned a disposition: accept, avoid, mitigate through controls, or transfer through insurance. All together, this is your corrective action plan. Now that you've done your math, here's the reality: once reasonable preventive controls are in place, an investment in impact minimization can quantitatively lower financial risk. This solution quantitatively reduces risk significantly more than additional investments in preventive measures that can never truly eliminate the full probability of an event. This may be pure business-speak, but, if you've done your math, you can prove what you say.

So instead of adding more controls in an attempt to prevent cyber incidents, you'd like to lower risk to the organization by integrating controls that address inevitable lapses in prevention. In risk management vernacular, your request for a detection and response service must hone in on how it **lowers that potential impact** by reducing **dwell time**[4] . MDR ensures compromises are eliminated within hours, and never reach the news or the regulators. In other words, MDR helps to put out grease fires in the kitchen before they burn down the house. [See Managing Risk to Reduce the Impact of a Breach[5] for additional detail.]

4. Communicate Full Scope of Potential Impact

In the event of a meaningful breach, you will find that insurance companies, regulators, shareholders, and customers may all get involved. The Federal Trade Commission may investigate whether public pronouncements regarding security match the actual practices of the organization, and negative findings could result in the FTC filing a claim of deceptive trade practices. Put quite simply—when a large-scale security event hits at a high-profile organization, it gets really ugly really fast, especially for the executives[6] at the top of the org chart. Furthermore, the reality is that ambulance-chasing attorneys lie in wait for the next "records breach" that leads to an unauthorized disclosure of protected information. The class-action suit literally follows 12 hours after the public disclosure of the event.

By using a simple approach[7] for the security program, risk tolerance is easier to establish with leadership. I've called out three outcomes to avoid: unauthorized disclosure of protected records, theft/extortion, and disruption of critical IT-based services. Left out of that discussion was the collateral damage that can occur, and how it may affect leadership very personally. If leadership is signing off to accept risk, they should be fully informed of the full scope of potential impact.

5. Highlight Opportunities for Cost Avoidance

Using the risk assessment results, you can now compare where you are paying for security technologies or human resources and where your actual security gaps are. You may see that you are spending money which you may be able to reduce or even eliminate. Those cost savings can help make an MDR vendor a budget-neutral decision.

Additionally, you may be able to replace expensive, existing technology if you subscribe to MDR. It is important to conduct your due diligence on preferred MDR providers. Although MDR does create several opportunities for cost redirection and avoidance, the specifics depend upon the MDR vendor you select. Here are a number of tools that may be included in your MDR solution and become

redundant:

- IDS and signatures
- Automated vulnerability-scanning
- SIEM
- Log retention and management

Additionally, there is an opportunity cost component to the savings that MDR drives. If your network engineer is spending 50% of her/his time to investigate security events from monitoring systems, you're paying for that time in the security budget already (whether or not it exists). While the engineer has a split focus, s/he isn't addressing security well, and their ability to keep IT projects on track or manage IT issues is weakened.

Secondly, from a security perspective, the critical investigation tasks will not receive the attention they deserve when an organization assigns responsibilities to multi-tasking IT staff. True breaches may slip through among the alerts.

Put simply, **if an IT team is also the security team, the chances of them doing a good job in either capacity is significantly diminished.** The analogy commonly used from the manufacturing industry is unplanned work[8] : one hour of unplanned, interrupt-driven work is cost-equivalent to two hours of planned work. Combining that cost with the certain opportunity cost[9] of delayed IT projects means that you may be significantly **overpaying for security and underachieving in terms of results.**

Less obviously, when IT staff are given security tasks, they receive extremely valuable security training while simultaneously experiencing multi-tasking that reduces job satisfaction. Considering that these employees will be overworked and, probably, underpaid, they will be likely to seek greener pastures and higher pay. The job market for security professionals is hot. Tasking IT staff with security tasks can lead to employee turnover; this is an artifact of market conditions that is potentially exacerbated by good intentions.

Example of cost avoidance calculation

- Cost avoidance opportunities
- % of time IT or security is spending tuning, investigating and responding
- Opportunity cost to IT transformation projects
- Cost of SIEM product (log management and “correlation”)
- IDS and signature costs
- Vulnerability scanning costs

Example Estimates (all costs annual)

50% of a network engineer spent on security	$90K for $120K engineer+load
10% slide in IT projects	$50K on a $500K project
Maintenance cost of SIEM*	$20,000 for $100K product
IDS signatures and maintenance on SourceFire*	$5,000
Vulnerability scanning	20% of cost of Qualys* (e.g.) $6,000
Total	**$171K**

*Financial figures may vary from vendor to vendor

Therefore, if the above numbers are reasonably accurate and reflective of a company, there’s about $150K to work with that would essentially make the transition to MDR zero cost, with the benefit of adding full SOC operations and recovering IT staff focus to digital transformation projects.

Costs for project slippage are generally well understood by project managers who are motivated to minimize those slippages – the above is a broad example. The bottom line is this—multi-tasking your existing IT staff results in you overpaying and underperforming on security monitoring, detection of nascent events, and rapid response to reduce dwell time. Fortunately, this is correctable.

Finally, if you have been requesting headcount to perform this function, using an MDR solution provider can help to avoid organizational expansion altogether, and provide an equivalent, auditable service at a fraction of the internal cost. If your own security organization experiences a lot of employee churn, the costs in additional HR engagement and recruiting costs are similarly avoidable.

CI Security™

6. Plan for a 1-Year Landing Strip

If these scenarios ring true for your organization, you probably have a 1-year runway to get your funding approved. Pick your preferred budget number and work toward it.

It's very likely that you'll have to prepare the ground far in advance of actually planting. As you develop your budget, you may have to consider biennial budget cycles (especially common in the public sector), existing 3rd party contracts, and the difference in availability for capital purchases versus a pure subscription service.

A reasonable way to come up with a number is to review pricing models for various vendors. CI Security™ prices by user, because we know that there is a fairly linear relationship between the number of users interacting with the Internet and the frequency of security events requiring investigation. Pricing varies on network and cloud models. For more information on pricing options for security operations, read Detection and Response: 4 Options for Security Operations[10] , where we've included specific information about the cost per user for managed detection and response.

Conclusion

InfoSec leaders are often challenged to create a compelling value proposition that can be reflected in budget. In order to address impact minimization through improvements in detection and response, successful leaders in Information Security have mastered the lexicon of risk management. By illustrating how detection and response (including a managed service) can significantly reduce the overall impact of foreseeable security events, leaders can help organizations build security operations that can handle evolving threat actor tactics, techniques, and procedures[11] while demonstrating the value of the investment.

info@ci.security
+1 206 687 9100
https://ci.security

CI Security™

Endnotes

1 **InfoSec Risk Management: a Primer to Assessing Technical Risk**, CI Security, April 2018, https://ci.security/research/infosec-risk-management-a-primer-to-assessing-technical-risk

2 **NIST Cybersecurity Risk Assessment Template**, CI Security, January 2018,

3 **Self-Assessment Questionnaire A (PCI-DSS SAQ)**, PCI Security Standards Council, https://www.pcisecuritystandards.org/pci_security/completing_self_assessment

4 **2018 Cost of a Data Breach Study: Global Overview,** Ponemon Institute, May 2018, https://www.ibm.com/security/data-breach

5 **Managing Risk to Reduce the Impact of a Breach**, CI Security, June 2018, https://ci.security/research/managing-risk-to-reduce-the-impact-of-a-breach

6 https://www.businessinsurance.com/article/00010101/NEWS06/160719794/Target-case-a-cyber-warning-to-corporate-directors

7 https://ci.security/news/article/small-biz-simplifies-and-moves-the-needle

8 **"Planned Work Predominance: Contribution to the Bottom Line,"** Efficient Plant Magazine, May 2012, https://www.efficientplanmag.com/2012/05/planned-work-predominance-contribution-to-the-bottom-line/

9 **"Unplanned Work Is Silently Killing IT Departments,"** Computer World, April 2006, https://www.computerworld.com/article/2563263/it-management/unplanned-work-is-silently-killing-it-departments.html

10 **Detection and Response: 4 Options for Security Operations**, CI Security, June 2018, https://ci.security/research/detection-response-4-options-for-security-operations

11 **"Inside the Mind of a Threat Actor: Tactics, Techniques, and Procedures Explained,"** CI Security, February 2018, https://ci.security/news/article/inside-the-mind-of-a-threat-actor

CI Security™