Security ROI
in 2015

Huntsman®
Defence-Grade Security Platform

5 things to consider when estimating the ROI on cyber security.

In June 2015, one of Australia's top cyber police officers, Detective Superintendent Arthur Katsogiannis, stated that internet-enabled crime "poses the greatest challenge to law enforcement in the 21st century"[1]. Similarly, in the US, the former CIA and NSA chief Michael Hayden highlighted the challenges faced by governments and businesses in an interview in the Wall Street Journal[2].

They are both reflecting on what many organisations have already come to recognise: cybercrime is not only on the rise; it is here to stay.

Which means that an organisation that wants to stay one step ahead of the cyber criminals needs to invest in the best security they can afford.

Estimating the Return on Investment (ROI) of security investments is not easy. It involves measuring not only the costs avoided or reduced by preventing or detecting a breach – such as losing critical data, or a breach so bad that it affects the capitalised value of the enterprise – but also the intrinsic benefits of having a security solution.

The issue, of course, is that not all security platforms are created equal – some provide a far greater ROI. We're proud that Huntsman® is one of those.

Here, we discuss five key factors to consider when looking for maximum ROI from a security platform.

Security ROI involves difficult questions:

- How do you calculate the value of improving organisational security and ensuring it complies with internal policies and external regulations?
- How do you assess the impact of a breach that you successfully prevented?
- What is the cost of a clean-up operation you didn't have to do?

1. CHOOSE HOLISTIC SOLUTIONS OVER POINT SOLUTIONS

When comparing security solutions, you will inevitably face the choice of point solutions – which address specific threats – versus security platforms that meet broader strategic security objectives, for example flexibility and scalability, like Huntsman®.

Our advice is to look long term. The ROI from point solutions can be negligible, and even offset by the extra time required to learn, configure and operate the solution. Point solutions also expose organisations to a continuous battle to deploy additional solutions to counter subsequent families of threats that emerge with immunity in the future.

In contrast, a security platform like Huntsman® provides value that is greater than the sum of its parts.

2. GET HARD NUMBERS FOR KEY METRICS

To justify spending more on security, you need hard numbers for key metrics such as:

- Total cost of ownership including the support of the security solution;
- Effective savings from reducing IT risk exposure;
- Compliance management efficiencies in remediation and audit;
- Reductions in future staff needs or costs, and benefits from staff redeployment; and
- Reduced costs through being able to phase out older technologies or processes.

3. INCLUDE RISK-ADJUSTED COSTS AND BENEFITS IN YOUR CALCULATIONS

When translating IT security and operational improvements into tangible figures, your business case must factor in risk-adjusted costs such as:

- The impact of a security breach on system downtime and productivity;
- The cost of losing (or restoring) valuable IP or confidential data;
- Any hard benefits attributable to improved risk management or corporate governance, like risk profile, cost of capital or credit rating;
- Penalties or fines for non-compliance with government and/or industry regulations; and
- The cost of investigation, remediation, clean-up, communications and recovery (including end customer costs).

The calculations typically assign probabilities to risks and estimate the costs of their impacts. So a security solution that makes a risk less likely to occur, or reduces its impact, can show a benefit from the 'unprotected' state.

Your business case should also account for common factors that are not part of the ROI justification but are clearly beneficial. These include benefits delivered by:

- The ability to visualise activity and systems usage across the enterprise to anticipate security issues;
- Real-time monitoring and control (as against periodic or ad hoc processes);
- The constant provision of information on compliance status (or a failure to comply); and
- The time freed up for security staff who no longer need to deal with issues manually, or resolve actual or potential security breaches, and the potential to use more junior or less experienced staff to monitor security.

4. CONSIDER WIDER COST FACTORS

Your business case should also include wider cost factors.

These can include the level of scalability or flexibility of a solution as an enterprise grows. Most organisations accumulate point solutions over time and accept the costs and inefficiencies of integrating and managing discrete systems or leave them to be managed separately within their respective silos[4]. But these systems can represent a poor investment.

Superior ROI can come from security systems that reduce those costs by:

- Integrating information from existing security solutions to provide a broader perspective;
- Reducing the time spent by staff cross-referencing and managing existing solutions;
- Eliminating duplication in security collection, analysis and interpretation;
- Providing sufficient modularity and scalability (thus avoiding the need for constant technology upgrades to deal with increasing data volumes);
- Integrating and solving workflow and process issues (and not creating new ones); and
- Intelligently and dynamically investigating and resolving threats, rather than just identifying them.

The greatest ROI will come from an approach to security that enables easy integration and inter-operability throughout the collection, analysis, monitoring, and reporting process.[4]

5. START SMALL AND GROW INCREMENTALLY

If the ROI case for a new security solution is tough to make, you should probably think about starting small. Begin with a project that will produce a measurable business benefit that can then be used to build a stronger, evidence-based business case for wider rollout, deployment or expansion. This way, you can keep security simple and manageable.

If you choose this path, then your assessment of value should include:

- The ability to phase deployment and expansion of the security solution;
- The benefits of removing information silos and integrating all data into a single point for security, compliance, monitoring and control;
- Savings in existing solutions or reductions in exposures that reduce the likelihood of loss (insurances, for example); and
- Process efficiencies and operational benefits from more intelligent security operations.

SUMMING UP

It is now widely recognised that organisations need a holistic approach to cyber security.[5] This can only be achieved with a systematic framework that can be easily managed.

Intelligent security investments that fit these criteria enable organisations to improve security and compliance, monitor corporate and IT assets more effectively, and lower the operational costs of those activities. This significantly strengthens the ROI case for their adoption in a way that is clear to business leaders and budget holders as well as technical security teams.

REFERENCES

1 The Sydney Morning Herald, June 16, 2015

2 Wall Street Journal, June 21, 2015 - http://www.wsj.com/articles/michael-hayden-says-u-s-is-easy-prey-for-hackers-1434924058

3 Aberdeen Group Research Brief – The Role of Security Information and Event Management (SIEM) in Security, Governance, Risk Management and Compliance (GRC)

4 Ibid

5 5 Steps to a More Secure Data Center, Enterprise Systems http://esj.com/Articles/2009/12/08/Secure-Data-Center.aspx?p=1

Huntsman | Tier-3 Pty Ltd

Asia Pacific

t: +61 2 9419 3200
e: info@huntsmansecurity.com

Level 2, 11 Help Street
Chatswood NSW 2067

EMEA

t: +44 845 222 2010
e: ukinfo@huntsmansecurity.com

100 Pall Mall, St James
London SW1Y 5NQ

North Asia

t: +81 3 5809 3188
e: info@huntsmansecurity.com

TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

Americas

toll free: 1-415-655-6807
e: usinfo@huntsmansecurity.com

Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com linkedin.com/company/tier-3-pty-ltd twitter.com/Tier3huntsman