IDC TOPLINE

HOW TO IMPROVE YOUR ABILITY TO RESPOND TO A BREACH THROUGH A PROACTIVE APPROACH TO CYBERSECURITY

Author:

Claudio Stahnke

September 2020

Sponsored by IBM Security

IDC #146760020

How to Improve Your Ability to Respond to a Breach Through a Proactive Approach to Cybersecurity

Introduction

Cybersecurity teams constantly deal with an ever-evolving threat landscape and are now being tasked with enabling companies to operate smarter. This means embedding security into the company culture, proactively linking security to changing line-of-business priorities, and enabling business outcomes. It also requires the implementation of proactive threat life-cycle management that enables digital transformation while improving client experience, protecting brands, building trust, improving competitiveness, and minimizing risk.

AT A GLANCE

KEY STATS

- Cybersecurity is seen as a business enabler by 63% of enterprises.
- 42% of enterprises already include cybersecurity in the planning of all new deployments.
- Hard-to-manage cybersecurity portfolios are the main inhibitor of security capability improvement.
- Despite the decrease in IT spending caused by COVID-19, 83% of enterprises have no plans to reduce their cybersecurity budgets.

As remote working assumes greater traction, responsive CISOs are enabling this shift, facilitating rapid cloud adoption, and lowering the risk from email-related vulnerabilities through training and awareness campaigns. IDC research shows that while 38% of enterprises expect to reduce their IT budget in the next two years, 83% will maintain or increase their security spend. How can security teams spend this money wisely, and how can they use it to further strengthen their corporate support and business alignment?

This IDC Topline discusses the steps that companies can take to improve their resilience in two key areas. On one hand, by focusing on measurable outcomes. On the other, by looking at how the right culture within an organization can further enhance the cybersecurity stance.

Reaching Measurable Outcomes

The skills gap: As the cybersecurity industry has faced a crippling skills gap since its inception, with no solution in sight and with the creation of hybrid environments only complicating things further, enterprises are pushed toward outsourcing their cybersecurity to service providers that can provide the right talent.

Incident response (IR) retainer: Considering the lack of internal resources to tackle attacks that could disrupt normal operations at any time, it's important to be able to rely on professional technical aid that can be delivered quickly in case of emergency. Securing this kind of fast support is paramount as it will help prevent a breach from having potentially catastrophic repercussions both in terms of data loss and reputational damage. As costs often rack up by the second following a breach, being able to deploy a quick response and reduce the mean time to

response (MTTR) can be extremely beneficial, making IR retainers very appealing, especially from a return on investment (ROI) perspective.

Basic IR retainer offerings are an inherent reactive measure, just like calling 911 after burglars have entered your house. More advanced IR services include elements that can help end users to prepare proactively to threats. For example, IR playbooks and IR rehearsals for employees will improve the overall response capability to address potential breaches. Other proactive elements can include assessments to IR plans with recommendations on how to improve them and utilize advanced tools and processes (such as threat intelligence). Specialized training can be provided for first responders within the organization.

Threat intelligence: The first step is to be aware of the threats that are out there. This is easier said than done, as methods of attack are always evolving and adapting quickly to new defense measures. Being able to rely on strong threat intelligence (TI), constantly updated through a vast network of sources that keep feeding the system with new threats, can help protect an organization from falling victim to new attack vectors. A strong threat intelligence foundation can help deploy the right policies as soon as a new menace is detected "in the wild" across the span of the network, creating a preventive system that protects organizations from breaches.

Strong threat intelligence also provides defenders with actionable insight on how attacks are executed. This enables overstretched security analysts to prioritize their response and operate more effectively, reducing the mean time to detect (MTTD) and MTTR.

Risk assessments: It's equally important to know what the internal risk posture is and to determine the risk level. Given that every reality is different, enterprises can have various levels of "acceptable" risk. It's important to engage with business stakeholders, as these should be involved in — or in fact determine — the decision. The main challenge is that executives and security specialists often struggle to communicate with each other, making the role of the CISO vital in bridging the terminology and language gaps. CISOs must articulate in business terms the likelihood and impact of a given event, and help the business decide how to mitigate these risks. This risk-based approach will help the CISO to communicate effectively with the board, by understanding what their risk appetite is and how security can be aligned accordingly. To achieve this, there's a need for continuous demonstration of the impact and progress of the security program, using interactive and visual reporting (such as dashboards) that can provide the board with metrics that are meaningful to the business.

Threat life-cycle framework: Implementing a comprehensive framework when creating a security portfolio will help to shape an environment that does not just protect against threats but also enables a more proactive stance. A proper assessment of what tools are needed will streamline the security environment, relieving overstretched personnel and increasing the overall ROI of security investments. The implementation of threat life-cycle management services such as threat intelligence and managed detection and response (MDR) will also drive further efficiencies, as they extend visibility over the entire environment, helping the cybersecurity team to focus their attention on the issues that matter most. Furthermore, access to a broad range of real-time TI, based on efficient network visibility and a breadth of data sources, will enable early

detection and facilitate threat hunting, switching the overall stance from reactive to a proactive search of potential threats within the environment.

These ambitions are critical when considering the context of enterprises pursuing digital transformation strategies that have been accelerated as companies prepare for the next normal. While this may result in a growing exposure to risk, security cannot afford to slow down, or stop, such plans. Rather, the goal must be to enable these initiatives, but securely. Hence the importance of cyber resilience — adopting the right approach to security operations that can drive a proactive approach to threat management. This in turn enables the enterprise to pursue digital transformation strategies without having to worry about the security implications.

Increasing efficiency: The main obstacles to delivering a better ROI on security investment are understaffing and a lack of automation. Adopting automated solutions can be particularly challenging in some cases, with the risk of overlooking indicators of compromise (IoCs) in environments that rely heavily on AI. This, together with the lack of skills, means security teams need to find and rely on partners that can deliver the right kind of support and help in the deployment and management of new tools.

Security automation promises improvements in efficiency, saving time for analysts, especially on low-value tasks such as integrating and operating disjointed security tools. The importance of rebalancing the workload for security analysts cannot be overstated as the industry remains plagued by a crippling skills gap. Burnout among security specialists is one of the main reasons why enterprises lose valuable analysts, so being able to retain scarce, talented experts is a top priority. Dedicating an adequate budget to training is fundamental in retaining employees, as effective and mature training programs will upskill current employees, opening new career paths within the organization and driving efficiencies.

Automating low-value tasks provides an opportunity to focus manpower on more value-additive, proactive activities. This reduces the need for new hires and adoption of further security tools, reducing overall expenditure. The adoption of MDR services, powered by AI, will make threat hunting a vital, proactive part of security. Externalizing such services will help the internal analyst team focus only on more qualitative tasks, increasing value and further reducing the risk of burnout.

Creating the Culture of Security

Embedding security in the new normal: As the world slowly moves to a next normal, now is the right time to push for new approaches to cybersecurity within the organization. Many enterprises have taken the opportunity brought about by reduced load and usage of IT systems to overhaul their IT systems, including embedding security measures into the new deployments, as highlighted by a recent IDC survey in which 42% of respondents said they include security in the planning of all new projects.

Training: It's equally important, though, to "embed" cybersecurity in the employees' culture in terms of how they approach their daily activities. Taking advantage of slowed operations,

organizations can dedicate time to training and retraining the workforce to adopt best cybersecurity practices.

Creating an IR plan: When retraining the workforce, it's paramount to reach beyond the security team to create a culture of cybersecurity that encompasses the whole organization. To achieve this, an IR plan needs to be created. This must be tailored, firstly, on the specific organization, with awareness/training and incident management response. Secondly, every department and area of the business should be able to rely on personalized guidelines as different employees will have to adopt different measures — personnel in the legal department, for example, will need to adopt different cybersecurity best practices from someone in marketing. Doing so will create a proactive environment in which employees will be less likely, for example, to fall victim to phishing campaigns, which remain one of the main vectors for threats.

Creating new guidelines, however, is not enough, as the risk of breaches persists. Every member of the organization needs to know what they are supposed to do in case of a successful attack. This will help drive down MTTRs and this is achievable only through continuous testing, training, and rehearsal of the IR plan. Creating and effectively implementing an incident response plan will greatly improve the organization's response and readiness. This, in turn, will help to reduce the impact that breaches can have on an organization. This is even more relevant when considering that the costs of a breach, together with the fallout on brand image and reputation, rise dramatically as the time passes after an attack.

Trickle-down cybersecurity: To effectively reach the different business lines within an organization the security team should focus first on involving executives from different departments, conveying the cybersecurity message in terms they can understand. Being able to translate the threat landscape into the context of how the business operates is essential. When framing the importance of triage and prioritization, for example, it's important to show how this can reduce the duration — and the consequences — of a breach, as this will lead to tangible ROI.

Risk is the language that bridges the gap between security experts and executives. Framing the discussion around risk, the security team should position itself as a risk advisor rather than just a security manager, demonstrating how security risk is enterprise risk and how proactive security teams can enable business outcomes (such as lower business risk and associated costs). Once executives are on board with the new cybersecurity strategy, the right culture will flow more efficiently within the organization.

Conclusion

The path to cyber resilience encompasses many different aspects for organizations, and no two strategies are the same. It is paramount to define an approach that fits the specific needs of the enterprise, addressing the achievement of measurable outcomes and creating the right culture within the organization. These approaches are two sides of the same coin, and no strategy can be successful without involving both — one provides the right measurable KPIs and the other the right mindset to take full advantage of the opportunities that an efficient cybersecurity strategy can provide, creating a system that will protect and be cost effective.

MESSAGE FROM THE SPONSOR

Many organizations lack the ability to identify, investigate, and respond quickly to cyberattacks. Organizations may not have response plans in place, or those plans may be untested, leaving the organization unprepared for an attack when it happens. Cyberthreat intel is misunderstood and under-utilized, and organizations often don't have the resources or expertise to respond effectively to malicious attacks. This means they're at risk of significant financial, business, and reputational loss — and may not even be aware of how significant the risk exposure is.

IBM helps organizations to prepare for, prevent, detect, and respond to security incidents efficiently, expediently, and with care toward their customers and networks. In a cyberattack every second counts. IBM offers threat intelligence, incident response, and strategic remediation to help organizations achieve better control over attacks and breaches. Your board and your customers expect your response to be swift and strong. While there is risk, there is also opportunity to be a leader in your industry and to show your values in action.

To learn more about IBM's incident response and threat intelligence services visit: ibm.biz/X-Force

About the Analyst

Claudio Stahnke, Senior Research Analyst, IDC

As a senior research analyst, Claudio Stahnke focuses on the security services market in Europe. He is based in London and works in IDC's European Security team. He engages with clients, answers inquiries, and delivers tailored updates focused on market opportunities. He also attends industry conferences and takes part in live broadcast interviews to discuss the latest trends in the security space.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Global Headquarters

5 Speen Street Framingham, MA
01701 USA
P.508.872.8200
F.508.935.4015
www.idc.com

Copyright and Restrictions