FORRESTER®

For: Security &
Risk Professionals

Rules Of Engagement: A Call To Action To Automate Breach Response

by John Kindervag and Stephanie Balaouras, December 2, 2014

KEY TAKEAWAYS

In A Post-Target-Breach World, Stopping Breaches Is A Business Priority

On December 18, 2013, Target publicly announced that it had been the victim of a major data breach that affected approximately 110 million customer records. As a result of the breach, the CIO and CEO lost their jobs, and to date, the breach has resulted in cumulative expenses of $146 million.

The Business Must Empower Security To Stop Breaches

Understanding the business' objectives and convincing the business to empower security professionals to properly respond to a possible data breach must be the near-term focus of security teams. In the post-Target-breach world, CEOs and boards now care about security more than they ever have before and worry about the potential impact of a breach to the company.

Automation Is The Answer

Given the consequences of data breaches, businesses can no longer rely on passive, manual procedures to defend against them. The only way to protect the exfiltration of our data by hackers and cybercriminals is to provide our security teams with a set of rules that will incentivize automated response.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617.613.6000 | Fax: +1 617.613.5000 | www.forrester.com

Rules Of Engagement: A Call To Action To Automate Breach Response

Processes: The Security Architecture And Operations Playbook

by John Kindervag and Stephanie Balaouras
with Glenn O'Donnell, Heidi Shey, and Claire O'Malley

WHY READ THIS REPORT

It seems that not a day goes by that there isn't another massive security breach in the news. Consumers around the globe hear about continual threats to their personal data while name brand retailers and enterprises are spending millions to respond, remediate, and recover from the theft of sensitive customer data and intellectual property. As the costs of data breaches skyrocket and regulators add more compliance burdens to the enterprise, the security industry must find new ways to more comprehensively meet these threats and prevent the exfiltration of proprietary data into the hands of cybercriminals and other malicious actors. This report is a call to action for a more automated threat response process based on developing a set of cyber "rules of engagement" that will empower security and risk management professional teams to act more quickly and aggressively to stop data breaches before they can threaten the business. This is an update of a previously published report; Forrester reviews and updates it periodically for continued relevance and accuracy.

Table Of Contents

Notes & Resources

This report analyzes recent cybersecurity attacks to provide S&R management professionals with valuable insights regarding the steps they should take to treat and avoid these problems from occurring in the future. Specific breaches that are addressed in this report include the 2013 Target and 2014 Home Depot hacks.

Related Research Documents

The Cybercriminal's Prize: Your Customer Data And Competitive Advantage
August 6, 2014

Targeted-Attack Hierarchy Of Needs, Part 2
July 24, 2014

IN A POST-TARGET-BREACH WORLD, STOPPING BREACHES IS A BUSINESS PRIORITY

On December 18, 2013, Target publicly announced that it had been the victim of a major data breach that affected approximately 110 million customer records including the breach of 40 million credit card numbers. This breach has had a seismic effect on global business for several reasons:

- **The CIO lost her job.** Beth Jacobs, who had been the CIO of Target since 2008, resigned her position as a result of the data breach.[1] Traditionally, CIOs have kept their jobs post-breach. If business executives need to blame anyone, it's usually its information security leaders. Sadly, for this CIO, there was no CISO at Target to take the fall.

- **The CEO lost his job.** Gregg Steinhafel, who had been with Target for 35 years, was let go in the breach's wake. According to a press release from the board of directors: "Most recently, Gregg led the response to Target's 2013 data breach. He held himself personally accountable and pledged that Target would emerge a better company."[2] We have entered a new era where investors and boards of directors would hold top business executives responsible for data breaches.[3]

- **The costs were astronomical.** According to Target's 10-Q, filed August 2, 2014, "Since the Data Breach, we have incurred $236 million of cumulative expenses, partially offset by expected insurance recoveries of $90 million, for net cumulative expenses of $146 million."[4]

The Target breach is the game changer. The replacement of two of the company's most senior executives because of the breach signals a new era, and we are in year 1 AT (After Target).

This new age offers a tremendous opportunity for security professionals. It's an opportunity to align with, and be empowered by, the business. It's also an opportunity to demand newer, better, and more-effective security controls. And, most importantly, it's an opportunity to automate security to become more dynamic and agile in the face of infinitely more sophisticated attackers.

But Security Teams Lack The Agility And Speed To Stop Devastating Breaches

Hackers don't have change management. For anyone ever involved in a data breach, this statement is self-evident. Hackers and other malicious cyberactors have the ability and freedom to hammer relentlessly at your digital assets — your networks and devices — to achieve their goal: stealing your data. They don't have the kinds of processes that can encumber business during an attack, and they are always moving much faster than the enterprise ever could. The most significant issue security teams face today is the lack of speed and agility in responding to a suspected data breach. Why do they lack speed and agility? Well, it's because security teams:

- **Lack the right tools in place to detect data breaches.** Traditionally, business technology (BT) leaders have been much more concerned with the availability of business apps and the network than with data security. As a result, many security teams lack tools such as database activity monitoring, endpoint visibility and control (EVC), and network analysis and visibility (NAV) that help identify anomalous behavior across apps, endpoints, and the network.[5] Most security teams are not in a position to either know about or respond to a data breach until it's too late.

  In fact, most enterprises and their security teams learn of the breach by a third party. In the massive Home Depot breach, the company reported: "The morning of September 2nd, our banking partners and law enforcement notified us of unusual activity connected to our payment systems."[6]

- **Lack the business mandate to proactively stop suspected breaches.** Even if security professionals detect a potential data breach, the business has not empowered them to actually shut it down. The first step that they must perform is breach validation — is this real or not? By the time they complete a forensic data breach validation the attackers have already absconded with your valuable data. This is why most security teams deploy their data loss prevention (DLP) solutions in passive mode. Their worry that they might block a legitimate business email with an attachment that contains sensitive data (even if it violates policy) far outweighs their worry of data exfiltration.

TO STOP BREACHES, SECURITY TEAMS NEED RULES OF ENGAGEMENT

To fight on the 21st century cyberbattlefield there must first be a new set of "rules of engagement." Whenever an organization suffers a breach, there is a sense that this is the first time anything like this has ever happened. Lack of preparedness when it comes to incident response (IR) plans contributes to this pain. While there may be an IR plan in place, it's rarely tested under battlefield conditions. A recent study highlighted that 23% of firms have not updated their IR plan in more than five years, and 46% of organizations actually test their plans.[7] By the time an IR plan is activated, it's too late. A breach has already occurred. IR is vital, but at the end of the day, it's still an exercise in clean-up. It doesn't stop a breach from happening.

On a real battlefield, all the combatants have received a set of rules of engagement, or ROE. The ROE defines what a soldier can or cannot do in a given set of circumstances. This allows an individual soldier to take appropriate action without going up the chain of command. However, on the cyberbattlefield, the exact opposite situation exists; there are policies, processes, and procedures which inhibit the ability of a cybercombatant (AKA the security pro) to take a needed and appropriate action. Operational activities, which are critically important in benign times, such as change management and configuration management, can actually hinder an effective, immediate response. If a security pro suspects a privileged employee of downloading sensitive data from a production database, it would be much more effective to immediately change or suspend that employee's privileges, as opposed to waiting for days to conduct an investigation and then request the change.

Establishing a set of policies — the ROE — empowers security employees to immediately respond to a possible data breach and potentially stop it before it can dramatically and negatively affect the company.

ROE Requires A Focus On Data Exfiltration, Communications, And Declarative Security

Understanding the business' objectives and convincing the business to empower security professionals to properly respond to a possible data breach must be the near-term focus of security teams. In the post-Target-breach world, CEOs and boards now care about security more than they ever have before. They worry about security and the potential impact of a breach to the company.[8]

Unfortunately, third parties discover most breaches; it's rare that the breached entity discovers it themselves. As discussed earlier, a lack of the right detection technology is a major part of the problem, but it's also because security teams do not look for data breaches, they look for attacks. While an attack may provide some evidence that a data breach is more likely — what the industry refers to as an indicator of compromise (IOC) — it is not a data breach in and of itself. To help identify breaches, ROE demands:

- **Identifying data exfiltration.** A data breach only occurs when a hacker or malicious insider exfiltrates regulated or sensitive data (what we refer to as "toxic data") from the enterprise's networks or applications.[9] When security teams focus intently on identifying and preventing attackers trying to get into the enterprise, many become too distracted from looking for toxic data leaving the enterprise. Additionally, a focus on attacks versus exfiltration can give security teams a false sense of security if they feel they are preventing most attacks.

- **Stopping data exfiltration.** The modern security organization must also place equal focus on detecting and stopping the exfiltration of toxic data into the hands of malicious actors. To do this, security teams must shift from an exclusive focus on attacks to a more balanced focus that also places the appropriate attention on data exfiltration. Although prevention isn't dead, it can and will fail.[10]

- **Communicating a strategic vision to leadership.** A recent study found that close to a third of security teams never speak to leadership, and of those who do, 23% say they speak to business executives only once per year.[11] It's important that security professionals take advantage of this new era and work to build a better relationship with the business. To do this, security policy must help achieve business goals. Unfortunately, security pros have often made security policies outside of the business. This is a problem because business leaders just assume that everything is fine, but when suddenly there is a breach, everyone is surprised. The shock comes because there is an over-reliance on outdated policies that don't work in our new data-centric, digital business environment. Policies don't fit the security needs of the business, and security pros must remedy this.

- **Engaging in declarative security.** Declarative security is the concept that the business drives the security objectives. The business will declare its desired security state by identifying compliance initiatives, data protection priorities, brand protection parameters, or sensitive intellectual property. It declares a set of priorities in order to develop a protection or response threshold and define the boundaries determining when security teams can stop data exfiltration without going through massive red tape.

AUTOMATED RESPONSE THROUGH ROE IS THE FUTURE OF SECURITY

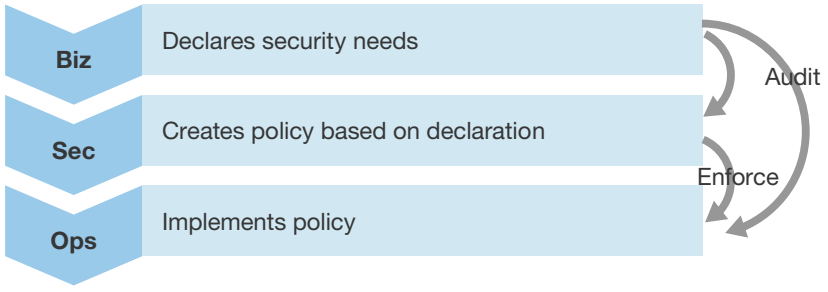
The only way to meet the declaration of the business and prevent the exfiltration of toxic data is to automate the response to a breach. The level of systemic complexity has increased to the point where manual response by security analysts is too difficult and ineffective. In the past, it was important to have a significant manual component to system configuration, but in fact, human error such as misconfigurations cause a significant portion of network downtime and security flaws. There is often a bias against automation, but the maturity of systems is such that truly achieving a valuable and reliable level of automation is now achievable.

Define Policy To Automate The Response

We must change our mindset about automation. When a human makes an error that causes a network outage or a security incident, we're very willing to forgive that person as we stand by the old "only human" adage. Unfortunately, we are much less willing to forgive an automated tool if we perceive that it has "made a mistake." Of course, any computation system is only as good as its inputs. And this is where leveraging our business' security declaration comes in. By translating a declarative security statement into an actual control policy, we ensure business and security alignment.

In this environment, the business will declare a security state, the security team will translate it into policy, and the operations team will implement the policy on the controls. This system provides multiple levels of audit and enforcement (see Figure 1).

Figure 1 ROE Diagram



87221 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Follow The ROE Workflow

Forrester has developed a workflow that demonstrates how security teams might translate ROE into actual control objectives. The interaction between the declarative statement, the security policy, the data, and the analytics engine will allow security teams to enter a new era of automation (see Figure 2). The elements of this workflow are:

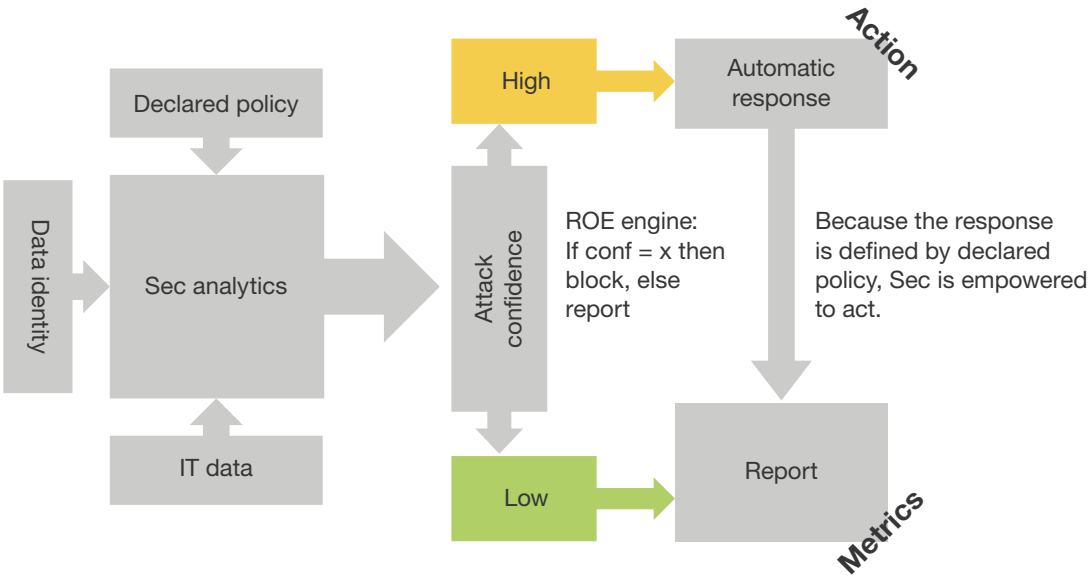
- **The declared policy.** This policy statement drives everything. Security pros translate the business declaration of security into a set of rules or configurations that can be used by the analysis engine central to the ROE system.

- **IT data.** Digital assets give off digital exhaust. Digital exhaust is the log, flow, and metadata that are a byproduct of the digital age. Adding IT data to security analytics provides the raw information needed to begin the ROE analysis. We must collect as much data as possible in order to have the information needed for the automated system to be functional and useful.

- **Data identity.** Data identity is metadata about the data itself, such as its classification, that must be persistently embedded into the data.[12] It's important to understand that data must travel with identity attributes so that a control can identify the data that it needs to protect from being maliciously exfiltrated.

- **The security analytics tool.** Security analytics (SA) is more than just the implementation of a security information management (SIM) tool. It includes not only the collection and correlation of traditional network and sys log data but also the integration of new types of security and IT data from across the digital business, such as feeds from NAV tools, alerts from DLP tools, behavioral analysis from IAM tools, and threat feeds from various security vendors and providers.[13] The declared policy, IT data, and data identity information are all fed into the security analytics tool in order to create a response index.

Figure 2 Define Policy To Automate Response



87221 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Create A Response Index

In order to know how to respond, Forrester has developed the concept of a "response index" that will define the ROE system's level of confidence that a potential security event such as a data breach is indeed happening. By leveraging a security analytics engine that generates a response index, a security team can automate the right type of response because there is an actionable metric regarding the system's validation of an event.

A response index works by computationally determining which events are most important and most likely. It does this by measuring a confidence level on the vertical axis and impact level on the horizontal axis (see Figure 3). Not only are SA tools integrating more actionable data, they are integrating with other security controls in your environment so that you orchestrate and automate breach detection and response. Key vendors include BAE Systems Applied Intelligence, CSG, IBM Q1 Radar, Intel/McAfee Nitro, LogRhythm, and RSA Security Analytics.[14]

The business will define the appropriate response index metric for each event. For example, an organization might determine that it's best to take no action when the engine determines that an event is low impact and has a low confidence level. However, when the impact is high and the confidence level is high, then declared security policy should dictate that security controls stop or automatically block suspicious traffic. The business should determine the scale and thresholds that best fit their risk profile and appetite.

Figure 3 The Response Index

87221 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

RECOMMENDATIONS

SECURITY AUTOMATION IS INEVITABLE; TAKE STEPS NOW TO ADOPT ROE

Given the nature of threats and the consequences of data breaches, businesses can no longer rely on passive, manual procedures to defend against data breaches. The only way to protect the exfiltration of our data by hackers and cybercriminals is to provide our security teams with a set of rules that will incentivize automated response. The speed of breaches is so fast that no human can ever keep up, no matter how knowledgeable and diligent. The consequences are too great to not adopt more automated security responses. However, providing the environment for the rules of engagement approach to automate breach response is a significant cultural shift that will need to be carefully socialized throughout the organization. There are actions that security pros can take to begin developing an ROE-based security response:

- **Look for evidence of data exfiltration.** Protecting your customers' data should be your top security priority; as a security professional, you need to become customer-obsessed.[15] You need to shift and balance your focus from attacks to exfiltration in order to prepare your teams for adopting ROE. One way to do this is to look for evidence now that cybercriminals are already buying and selling your customers' data on black markets. You will also likely find evidence that some of your IP is for sale on black markets.

- **With evidence of data exfiltration in hand, find a business champion.** It's imperative that business leaders understand and advocate for the pivot to a more automated, ROE-based security posture. Showing them evidence of data exfiltration is a very tangible way of proving just how important it is to automate breach response. It's helpful to recruit the CIO, but finding a forward-thinking business leader who can promote these ideas throughout the leadership team is better. A business leader, like the head of customer experience or the chief customer officer, might be a great new ally because breaches undermine customer trust and loyalty in the company.

- **Work with business technology counterparts to define an ROE workflow for your organization.** Much of the work creating an ROE-based security posture is found in developing a set of workflows and processes. Your counterparts in infrastructure and operations (I&O) are a good place to start. Too often, I&O and security teams maintain separate network and security operations centers (NOCs and SOCs). When these teams are separate, each team maintains its own policies and purchases its own controls, and too often, these teams have conflicting priorities (availability versus security). By converging the operational aspects of the network and security teams into a single organizational unit, they can become more efficient and be in a much better position to define and then implement an ROE framework.

WHAT IT MEANS

ROE EMPOWERS SECURITY WHILE IT PROTECTS THE BUSINESS

Because the response is defined by declarative security, security teams are empowered to act. People in organizations are often worried about getting in trouble for taking action, so they frequently choose not to act at all. In the modern threat environment, not taking action is not an option. To combat the type of agile, fast, and dynamic threat actors we face today, the business must provide a set of rules of engagement that empowers security professionals to take the aggressive action necessary to meet aggressive threats.

Just as military rules of engagement both empower combatants and protect everyone on the battlefield, so too a cyber-ROE can incentivize employees to do the right thing to protect the business and keep toxic data out of the hands of malicious actors.

ENDNOTES

[1] Source: Howard Baldwin, "The Other Shoe Drops For Target's CIO," Forbes, March 11, 2014 (http://www.forbes.com/sites/howardbaldwin/2014/03/11/the-other-shoe-drops-for-targets-cio/).

[2] Source: " Statement from Target's Board of Directors," Target.com, May 5, 2014 (http://pressroom.target.com/news/statement-from-targets-board-of-directors).

[3] Source: Eric Basu, "CEOs Can No Longer Sit Idly By on Cybersecurity," Entrepreneur, May 16 2014 (http://www.entrepreneur.com/article/233911).

[4] Source: "sec filings," Target.com (http://investors.target.com/phoenix.zhtml?c=65828&p=irol-sec&secCat01.28_rs=1&secCat01.28_rc=10).

[5] From a technology perspective, there are four primary functions, or pillars, that are necessary for breach detection: 1) malware analysis; 2) network analysis and visibility (NAV); 3) endpoint visibility and control (EVC); and 4) security analytics (SA). For more information, see the July 24, 2014, "Targeted-Attack Hierarchy Of Needs, Part 2" report.

[6] Source: "FAQs," The Home Depot (https://corporate.homedepot.com/MediaCenter/Documents/FAQs.pdf).

[7] Source: Brian Price, "Incident Response Plans Lacking In Many Organizations: Survey," Security Week, September 18 2014 (http://www.securityweek.com/incident-response-plans-lacking-many-organizations-survey).

[8] And rightly so! Protecting customer data such as credit card information, log-in credentials, and other personally identifiable information is one of the top priorities for both security and risk (S&R) leaders and business leaders. And as the threat landscape continues to evolve, S&R leaders must adjust their risk management strategies to also counter the next frontier: intellectual property theft. This report investigates common ways that cybercriminals steal data from organizations today, the cost of breach, and what organizations must do to enhance cybersecurity and protect their valuable data. See the August 6, 2014, "The Cybercriminal's Prize: Your Customer Data And Competitive Advantage" report.

[9] Data defense is the fundamental purpose of information security. Forrester designed this report to help S&R leaders develop effective policies using our Data Security Control And Control Framework as a guideline. For more information, see the January 15, 2013, "Know Your Data To Create Actionable Policy" report.

[10] In this report, Forrester discusses the four technologies that should form the pillars of your breach detection capabilities: malware analysis, network analysis and visibility, endpoint visibility and control, and security analytics. For more information on breach detection and response, see the July 24, 2014, "Targeted-Attack Hierarchy Of Needs, Part 2" report.

[11] Source: Ashley Carman, "Report: 31 percent of IT security teams don't speak to company execs," SC Magazine, July 17, 2014 (http://www.scmagazine.com/report-31-percent-of-it-security-teams-dont-speak-to-company-execs/article/361263/).

[12] For an in-depth discussion of data classification see the October 1, 2014, "Rethinking Data Discovery And Data Classification" report.

[13] Forrester segments the problem of securing and controlling data into three areas: 1) defining the data; 2) dissecting and analyzing the data; and 3) defending and protecting the data. We refer to this as our Data Security And Control Framework. In this report, we offer more vision and detail for dissecting and analyzing data. Business executives demand data for decision-making. For more information, see the August 9, 2012, "Dissect Data To Gain Actionable INTEL" report.

[14] Automation is just one criterion to consider when evaluating SA solutions. For a list of SA selection criteria, considerations and vendors, see the July 24, 2014, "Targeted-Attack Hierarchy Of Needs, Part 2" report.

[15] Customers may not have been so concerned about data security in the past, but customer awareness is now at an all-time high, and data security and privacy concerns will increasingly influence customer buying decisions. For more information, see the September 17, 2014, "CISOs Need To Add Customer Obsession To Their Job Description" report.

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals