

# THE CRITICAL INCIDENT RESPONSE MATURITY JOURNEY

## **ABSTRACT**

Learn how to holistically assess and improve the maturity of your organization's critical incident response program.

December 2013

EMC WHITE PAPER



# TABLE OF CONTENTS

- ABSTRACT ..... 1**
- TABLE OF CONTENTS ..... 2**
- INTRODUCTION ..... 3**
- ESTABLISHING AN EFFECTIVE COMPUTER INCIDENT RESPONSE CENTER – IT’S A JOURNEY ..... 4**
- CRITICAL INCIDENT RESPONSE MATURITY FRAMEWORK ..... 6**
- HOW TO ACCELERATE YOUR INCIDENT RESPONSE MATURITY JOURNEY..... 9**
  - People ..... 9
  - Processes..... 11
  - Technology ..... 12
- RSA OFFERINGS THAT HELP TO ACCELERATE YOUR INCIDENT RESPONSE MATURITY JOURNEY ..... 13**
- CONCLUSION ..... 14**
- AUTHOR BIOGRAPHY..... 15**
- CONTACT US ..... 15**

## INTRODUCTION

I didn't know it at the time but my introduction to the security specialty of incident response occurred when I first read the book *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*, by Clifford Stoll. The book goes into great detail of how Stoll combined his general curiousness and computer expertise to ultimately catch a German based spy for the Soviet Union that was hacking the computers at the Lawrence Berkeley National Laboratory. Unfortunately, even today, too many organizations' incident responses are ad hoc processes often conducted by lone wolfs; today's Clifford Stolls.

Even in the general audience news these days we are flooded with reports of organizations in nearly every industry that have been breached and that have had to deal with both soft (brand/reputation) as well as multiple hard costs (emergency incident response/consulting, regulatory fines, and customer remediation) as a result. The Ponemon Institute estimated that in 2013 the average cost of a data breach in the USA to be \$5.4M.<sup>1</sup> One day it is hacktivists or internal attackers and the next day it is cybercriminals or nation states that are causing the breaches. What many organizations are currently doing for IT security just isn't working. Preventive security schemes alone have proven to be insufficient.

Dr. Anton Chuvakin an IT security analyst with Gartner states the need for more mature incident response quite succinctly in a recently published report, "...prevention and preventative security controls will fail. Prevention fails on a daily basis at many organizations; it will suffice to look at antivirus tools and contrast their 99%-plus deployment rates with widespread ongoing malware infection rates."<sup>2</sup> In the same report Dr. Chuvakin goes on to write, "Because they [organizations] are not paying attention to detection, they never know they are having an incident that they need to respond to. Some think they are being "proactive" by their exclusive focus on preventative measures and neglecting the monitoring and response (in reality, this is being shortsighted, not proactive)".<sup>3</sup>

I believe however that times are now changing. Computer forensics and incident response are now beginning to claim their rightful position as key sub-specialties of information security, becoming more professional with the application of sound engineering principles and human expertise. The need is certainly great. As has been well documented, cybercriminals, nation states, and hacktivists are only too willing to take advantage of the modern day's data and application explosion for their nefarious purposes.

This is why incident response is now emerging as a high demand security sub-specialty. Today in most organizations, security investments, including all areas of investment (covering people, processes, and technology), are way out of balance. The vast majority of security controls today are for prevention and not monitoring (detection & investigation) and response. RSA estimates that organizations in aggregate spend approximately 80% of their security budgets on prevention, with monitoring and remediation splitting the remaining 20%. Organizations have spent more than 10 years trying to firewall, anti-virus, encrypt, and authenticate themselves to an acceptable level of security. However, these preventive approaches simply do not greatly inhibit today's sophisticated, well-funded, persistent, and focused attackers. Organizations need to change (or really rebalance) their overall security defenses given today's realities. And leading (mature) organizations already recognize this and are explicitly changing their security investment to be more balanced.

---

<sup>1</sup> 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2013

<sup>2</sup> Security Incident Response in the Age of APT, Dr. Anton Chuvakin, Gartner, September 25, 2013

<sup>3</sup> Security Incident Response in the Age of APT, Dr. Anton Chuvakin, Gartner, September 25, 2013

Organizations appear to be starting to recognize the increased need for professionalized incident response capabilities as a key part of this defensive rebalancing. In fact in a recent Forrsights Security Survey executed by Forrester Research in Q2 of 2013, they found that 67% of organizations reported that improving their incident response and forensic capabilities was either a high or critical priority. And for organizations that were larger than 20K employees this percentage was even higher, coming in at 72%.<sup>4</sup> There does at least appear to be an awareness of the need and some impetus to make a change in investment priorities, the real question now boils down to, what, when, and how.

Organizations that have recognized the need for a new defensive balance have often crystallized this by focusing on their security operations centers (SOCs), computer incident response centers (CIRCs), or critical incident response teams (CIRTs) as an optimal organizational platform for improving their monitoring and response capabilities. Whatever name one chooses to refer to this security function by, what they all have in common is that they are the organization's command center for the detection, investigation, and remediation of cyber security incidents. They are a formalized and professionalized version of Clifford Stoll since they are the security organization that is in focus when preventive controls fail to prevent.

## **ESTABLISHING AN EFFECTIVE COMPUTER INCIDENT RESPONSE CENTER – IT'S A JOURNEY**

The remainder of this paper will focus on defining levels of CIRC maturity and on how your organization can continually improve your incident response capabilities to significantly reduce the probability of experiencing a damaging incident. While preventive controls aren't 100% effective, this does not have to mean that damaging breaches are inevitable.

The best way I have found to measure the level of maturity of an organization's CIRC is by considering its maturity against the three well established and tightly interrelated categories of: people, processes, and technology. Great technology in the wrong hands isn't a path to success for detection or response. And similarly great people without appropriate technology are at best highly inefficient and at worst are overwhelmed by data and incapable of consistently providing effective service. And finally, solid incident responders with solid technology, but having no well considered and established processes will thrash themselves to the point of maximum frustration and leave their organizations less than optimally defended. An effective and properly maturing CIRC requires all three dimensions – people, process, technology – to work well and improve together.

For the purposes of this paper I have established three levels of CIRC maturity:

- Ad hoc incident response (low maturity)
- Incident response as an emerging security function (medium maturity)
- Incident response as a key force in an organization's security defenses and risk management (high maturity).

---

<sup>4</sup> Forrsights Security Survey, Forrester Research, Inc., Q2 2013.

The purpose of this categorization is to help you to holistically assess the maturity of your incident response organization. But of course every organization is different. When reviewing this maturity framework and placing your organization in it, realize that you might not perfectly fit into one level of maturity in all three categories. Use this framework in combination with the concept of “preponderance of the evidence” to place your organization where it best fits in the three levels. But keep in mind that where you are going and how you are going to get there is much more important than where you currently are.

From my contacts with customers and prospects and from those of my colleagues here at RSA, and after also considering industry research on the topic, I estimate that for incident response maturity, approximately:

- 65% of organizations are “Ad Hoc”
- 25% of organizations are “Emerging”
- 10% of organizations are a “Key Force”.

So don't be too hard on yourself if you find your organization in the “Ad Hoc” or “Emerging” categories. You have a lot of company. The more important question to ask is what you can do today to move your incident response maturity needle in the right direction. While exactly how much your organization invests in incident response is a unique decision based on risk tolerance, scale, business objectives, and industry, the goal of a mature set of people, processes, and technology for incident response is universal.

The Critical Incident Response Maturity Framework below lays out many indicators of maturity. Find where your organization currently best fits and then move on to consider how your organization can improve its maturity along these categories. Finally, also consider how RSA can help. Don't think of RSA as purely a vendor of technology. In the area of incident response RSA offers a broad set of products and services, each of which tie back to holistically improving an organization's incident response program.

# CRITICAL INCIDENT RESPONSE MATURITY FRAMEWORK

	<b>Ad Hoc Incident Response</b>	<b>Incident Response as an Emerging Security Sub-Organization</b>	<b>Incident response as a <u>key force</u> in security defense/risk management</b>
<b>People</b>	<ul style="list-style-type: none"> <li>Incident responders are part timers/borrowed from other IT/IT security functions. They work on an as-needed basis only</li> <li>Incident responders are not specialists</li> <li>Limited formalized training available They are on their own to skill-up</li> <li>Incident response often requires “beyond the call of duty” work efforts</li> <li>Little governance or interaction with service providers. SPs often seen as just dumping alerts at the organization.</li> </ul>	<ul style="list-style-type: none"> <li>Has full-time incident responder(s)</li> <li>Has a full time SOC/CIRC manager</li> <li>Has a plan to use specialized service providers</li> <li>Uses general purpose threat intelligence, not specific to the organization</li> <li>Off hours coverage is provided by SP and/or on-call staff</li> <li>Regular training and IR community participation</li> <li>Somewhat specialized into areas of focus and expertise</li> </ul>	<ul style="list-style-type: none"> <li>CIRC team is divided into clear specialties</li> <li>Participate directly in hacker forums/social media</li> <li>Collect and analyzes threat intelligence that is unique to the organization</li> <li>Follow-the-sun coverage</li> <li>Has business/risk analysts as agents of the CIRC team that are connected to new IT initiatives to provide guidance on risks and critical IT assets are IR-enabled.</li> <li>Regular staff rotation to increase skills and reduce burnout</li> <li>Reporting in business impact language, not just in security/IT lingo</li> </ul>
<b>Process</b>	<ul style="list-style-type: none"> <li>Unclear how the incident response function fits into the overall organization</li> <li>Most investigations initiated as a result of “alerts” from 3<sup>rd</sup> parties/employees</li> <li>Focused on clearing alerts, without prioritization</li> <li>Tend to focus on external threats versus internal threats</li> <li>Heavily focused on meeting compliance mandates versus</li> </ul>	<ul style="list-style-type: none"> <li>Security &amp; risk, not compliance, drives program</li> <li>CIRC effectiveness not judged by qualitative or quantitative measures</li> <li>Prioritize responses for a predefined set of IT assets without regard to other context factors</li> <li>Often fixing/reimaging of systems, not on understanding root cause</li> <li>Have process for “declared incident” which triggers third party outreach</li> <li>Regularly cooperates with other functions (Legal, HR,</li> </ul>	<ul style="list-style-type: none"> <li>Clear visibility &amp; involvement with the key business priorities of the organization to make sure that they are effectively security/IR-enabled</li> <li>Success judged based on security posture relative to key IT assets/business initiatives</li> <li>CIRC effectiveness continually judged by both qualitative/quantitative measures</li> <li>Focuses on responding to highest priority alerts (based on asset value, vulnerability,</li> </ul>

	<p>enhancing security or protecting the business</p> <ul style="list-style-type: none"> <li>• Limited differentiation of protection based on asset value or a threats level of risk</li> <li>• What is a “declared incident” not defined</li> <li>• Response procedures not well documented</li> <li>• No one manager in charge of detection &amp; investigation of incidents</li> <li>• Organization doesn’t participate in threat intelligence sharing groups</li> <li>• Service provider has little understanding of business/risk context</li> <li>• Service provider not able to monitor the most important business initiatives</li> <li>• Has limited oversight/governance /engagement outside of security organization</li> </ul>	<p>business management)</p> <ul style="list-style-type: none"> <li>• CIRC part of regular security/risk posture reporting</li> <li>• Performance metrics collected and shared with the CIRC team &amp; others</li> <li>• Defensive focus balanced between internal and external threat actors</li> <li>• Regularly uses commonly accepted control frameworks (eg..ISO, COBIT)</li> <li>• Value of IT assets &amp; processes plays important role in prioritizing responses</li> <li>• Good technical and management coordination with service provider</li> <li>• Delegates to IT Operations for detection and remediation of mundane/well-known threats</li> <li>• Delegates management of commoditized security technologies (AV, Firewalls, Vulnerability scans) to less costly staff or service providers</li> <li>• Subscribes to threat intelligence services provides by security associations &amp; vendors</li> <li>• Has light, but direct participation in in threat intelligence sharing groups</li> <li>• Operationalization of threat intelligence is primarily done manually</li> <li>• Has some oversight/governance/engagement with other functions (legal, HR, IT, BU)</li> </ul>	<p>exploit, attacker) , not on just clearing large backlog of alerts</p> <ul style="list-style-type: none"> <li>• Aims to understand the full scope of an attacker’s campaign, not just clean malware</li> <li>• Operates with clear governance, and within established cross-functional team</li> <li>• Provides follow-the-sun coverage with staff or with a mix of staff &amp; closely coordinated service providers</li> <li>• Pre-existing guidelines for prioritizing incidents</li> <li>• Security in general &amp; CIRC in particular are well integrated into the organization’s risk &amp; compliance program</li> <li>• Takes active part in threat intelligence sharing within appropriate industry, country, and law enforcement groups</li> <li>• Has shifted from exclusively responding to alerts to hunting for security issues/anomalies</li> <li>• Clearly separated from IT operations &amp; basic security operations functions with established touch points and division of roles and responsibilities</li> <li>• Regularly conducts post-mortems on incidents and feeds learning into tools (preventive, detective, investigative, and response as appropriate) and IR techniques/processes</li> <li>• Threat intelligence operationalized directly into tools</li> </ul>
--	---	---	---

## Technology

- |  |  |   |
|--|--|---|
| <ul style="list-style-type: none"> <li>• Primarily use perimeter and signature-based security controls</li> <li>• Security tools primarily purchased to prevent specific types of attacks and are deployed in silos</li> <li>• No standard set of incident response tools</li> <li>• SIEM tool not effectively used for threat detection or investigations</li> <li>• No purpose built security incident management system. Typically use Excel, email, or general purpose IT help desk system</li> <li>• Don't incorporate external threat intelligence into detection/investigations</li> <li>• IT asset information and other business and technical context not easily available</li> <li>• No malware analysis</li> </ul> | <ul style="list-style-type: none"> <li>• Incident management system is built from generalized tools (Excel, Wikis, Sharepoint)</li> <li>• Early stage of building out documented incident response procedures</li> <li>• Using SIEM + Network Monitoring tools on key network segments to enhance visibility</li> <li>• Threat intelligence provided by external sources and at least partially integrated into monitoring system</li> <li>• Conducts majority of investigations with data on-hand in the incident responders' investigative system</li> <li>• Conducts malware analysis, but doesn't automatically filter or prioritize which malware to analyze</li> <li>• Basic compliance/governance reports generated from monitoring system</li> </ul> | <ul style="list-style-type: none"> <li>• Use specialized security incident management system with library of incident response procedures</li> <li>• Have integrated platform for detection, investigation, management, and response</li> <li>• Have comprehensive network packet-level monitoring on all Internet egress points and key internal network segments</li> <li>• Widespread log/event collection that is closely integrated with network-level visibility</li> <li>• Signature-less file monitoring for malware and anomalies on endpoints</li> <li>• Established malware analysis process which prioritizes analysis based on asset criticality, vulnerabilities, and attacker campaigns</li> <li>• Business/technical context &amp; vulnerability information readily available to analyst</li> <li>• Identity &amp; user entitlement information is readily available to analyst</li> <li>• Location of sensitive data is readily available to analyst</li> <li>• Regularly updated knowledgebase of threats, tools, techniques, and tactics.</li> <li>• Use consolidated "big data" security analytic warehouse (containing both structured and unstructured data) for detecting/hunting for security anomalies</li> <li>• Centralized management dashboard used to coordinate incident investigations</li> <li>• Able to conclusively determine what data has been</li> </ul> |
|--|--|---|

**Technology  
Continued**

exfiltrated

- Regular reports of CIRC performance and security posture of the organization
- Tracks specific metrics such such as average time to identify and remediate attacks, # of incidents responded to, # and cost of successful attacks, time/cost of unplanned remediation, and # of stolen identities

## **HOW TO ACCELERATE YOUR INCIDENT RESPONSE MATURITY JOURNEY**

Now that you have found where your organization is on its incident response maturity journey, the question you should be asking is how you can help drive your organization forward on each of three fronts (people, processes, technology) at the same time. The short answer is to create a plan. A plan which balances the three, invests incrementally, and goes out at least one or two years, beyond a single budget cycle. This plan will not be static. It will change and perhaps change a lot, in part based on actual experiences with incidents to which you respond. You must keep it current so you always know what you are trying to do at least one or two steps ahead of where you are. If this sounds like planning for “continuous improvement”, it should. It is important to keep in mind that the ultimate goal of an incident response team is to detect, investigate, and respond to incidents to stop them from becoming damaging breaches. It is not the goal of the incident response team to be the security clean-up crew.

For the remainder of this section I will provide general advice on how to improve the maturity of your incident response function across each of the three categories. For areas of particular focus please refer back to the Critical Incident Response Maturity Framework above.

### **People**

Particularly if you are in the ad hoc maturity category, you probably think that you just don’t have enough of the right people to fill the role of incident responder. You probably are right. In general, however, it is better to have one or two “rockstar” incident response analysts than many more general purpose security or IT people that do incident detection and investigation as an occasional part-time job. If you don’t have any rockstar security analysts currently, do you have one or two people on staff that have the potential and the desire to become one? If so focus your education and training budget on them. Send them to incident responder/analyst school and related industry events like Black Hat and Defcon, and give them relatively free reign to create what it means to be a CIRC analyst in your organization. Resist the temptation to divert them to other projects or to use them for more mundane security operations tasks. They are your hunters; don’t try to domesticate them.

If you find your organization from a people point of view more in an “emerging” CIRC maturity level, what you should focus on is further developing the specialization of your team. Define and create specific CIRC job roles such as tiers of analysts (two or three tiers should be enough) that deliver specialized investigative services such as: Tier 1 analysts - eyes-on-glass, initial alert triage, preliminary investigation and Tier 2 analysts – reverse malware engineering, host & network forensics, data exfiltration investigations. These front line CIRC analysts should be complemented by other specialists that are focused on collecting and interpreting threat intelligence, understanding active attacker campaigns, and on building out the detection, investigative, and response tools in use by the Tier 1 and 2 analysts.

In addition service providers can be contracted to be a key part of your CIRC to help fill gaps and lower the performance pressure on your full-time CIRC staff. MSSPs typically are best suited to supply Tier 1 analysts to complement your CIRC team as they require the least amount intimate internal knowledge or access to do their jobs. Service providers can also be contracted to provide occasional specialized services such as integration, tool customizations, performance tuning, alert definitions, custom analytics, malware analytics, and report generation.



### **SPECIALIZED ROLES IN A CRITICAL INCIDENT RESPONSE CENTER**

It is also important that these CIRC roles be defined in such a way that there is rotation and a career path among them, as one way to mitigate analyst burnout is to have job rotation built into your personnel strategy. Another advantage of a well-functioning team of specialists is that your team does not become excessively dependent on a single individual, and thus as people move-on outside of your CIRC, it becomes easier to insert new people to take up the slack, as the needed role is well defined.

In effect by following the “people” advice in this section you are helping to manage your incident response function more as a science than as an art and more as a team than as a set of lone wolves. Doing this well will also help the retention and recruitment of your CIRC staff, as the best want to work with the best.

## Processes

As your CIRC expands in terms of people, capability, and geography, how you operate becomes as important as what individual analysts are doing. Incident response teams are best considered as implementing continuous processes of detection, investigations, and response. Security issues continually flow through the organization as opposed to periodically arriving. The more the organization monitors the more that will be found that requires further investigation. However all issues cannot be dealt with with equal priority; the list of events will be too long. CIRCs need to come up with policies and procedures in part to help guide the investigations that the analysts conduct and can follow and refine as the organization gains experience and maturity. Also industry-wide incident response best practices exist, so why not use them? Look to leverage the best practices produced by NIST, VERIS (Vocabulary for Event Recording and Incident Sharing), and the SANS Institute, for example. To these industry frameworks your organization can add response procedures/run-books that are specific to your organization.

Given today’s state of near universal vulnerability to insider and external attacks it makes sense to work out investigative and breach response procedures in advance, among your CIRC team, your broader IT security team, as well as with the rest of your organization. Don’t wait until you have an actual breach to work out what you would do if you had a breach. Document these procedures and ideally enforce and automate them via appropriate IT systems. Similarly the management of actual incidents that require remediation should not be left up to “random acts of heroism”. The security organization should pre-define levels and types of incidents and come up with incident management policies (ideally also enabled with appropriate technology) to help prioritize and address security incidents.

As CIRCs mature they mature in a way that resembles a sports team. Whether you follow baseball, rugby, or American or European football, you will recognize that the best teams are made up of a set of specialists that when maximally effectively leverage the individual’s skills in a way that the effectiveness of the whole is greater than the sum of the parts. This doesn’t happen by accident. Each individual simultaneously needs to understand their individual role and how he complements the team that is around him. Said another way, each individual needs to fit into and contribute to the procedures that define the operations of the CIRC team.

And just like sports teams that continually measure the effectiveness both of individuals and the team as a whole on multiple quantifiable and qualitative measures, so must a CIRC. And these measures must be collected and evolved over time, with continual improvement as the obvious goal. Also like a sports team, practice must be taken very seriously. As professional athletes say, good performance in practice typically precedes good performance in the game. This is why maturing CIRCs regularly run breach readiness and response tests, simulated incidents and breaches, and often bring in outside experts to evaluate and benchmark them.

Finally, the CIRC should not operate without proper oversight and business integration. It should not be setup as a free-wheeling, unbounded internal monitoring organization. For example what employees are doing with their time online should be out-of-scope for the CIRC, as the CIRC should stay focused on protecting the business and not on reporting on potential employee time wasting. What is inbounds and out-of-bounds for the CIRC to detect and report-

on should be governed on an ongoing basis. In fact in many countries, such as Germany, France, and much of the rest of Europe, what type and level of monitoring CIRC can conduct is in part limited by data privacy, telecommunications, and other laws. And these data privacy and related laws are in a continual state of change and interpretation and thus so too must be the rules under which the CIRC operate.

## Technology

The critical third leg in any incident response program are the systems that are used by the security analysts and their management to execute their detective, investigative, response, and management jobs. With incident response, speed, efficiency, and effectiveness are the name of the game. But a key challenge is how to do this across a large swath of the organization, or even the whole enterprise, with a relatively small number of CIRC personnel. If your incident responders have to open tickets and call in personal favors to get access to the underlying security telemetry and other data that they need to do their jobs, they are starting way behind the curve.

What security analysts need is comprehensive and immediate **visibility** into the security relevant activity in their organizations. They need this visibility to both better detect as well as to more efficiently investigate activities and alerts that are key indicators of compromise. One important way organizations can improve their visibility that was suggested by Forrester Research, Inc. in a report by Rick Holland entitled *Seven Habits of Highly Effective Incident Response Teams* is by “reducing the Internet ingress/egress points within your environment or ensuring network visibility at each Internet point of presence...”<sup>5</sup> Other important forms of visibility, in addition to network level telemetry mentioned by Forrester, are logs and events from the underlying infrastructure, applications, and security systems that make up your IT environment. Finally, when dealing with malware, having immediate visibility of what is happening on particular hosts, also often proves to be critical.

But that is not all, security analysts also need **context**, both business and technical, with which they can prioritize their investigations as well as better execute their forensic evaluations. After all, how can analysts effectively do their jobs if they don’t know what an IT asset is, what it is used for, what vulnerabilities might exist on it, how critical the asset is, where it is, and other important elements of context?

And finally incident response teams need automation, in many forms, to accelerate what they do. The management of alerts, investigations, incidents, breaches, staffing schedules, threat intelligence, reporting, run-books, and risk registries, to name a handful of areas in need of automation, help incident response teams do more with less. These areas of automation help to leverage the human expertise which is in such short supply and that is often wasted on repetitive, manual tasks. While technology certainly isn’t the single solution to the challenges impacting incident response teams, when well used it can help organizations get the most out of their people, while minimizing the burnout of being in a constant “hero/fire-fighting” mode.

Some specific CIRC focused technologies that are used by maturing CIRC are: centralized log/event (SIEM) and network monitoring systems, threat intelligence (operationalized into your monitoring infrastructure), workflow, reporting, correlation, archiving, big data analytics, host forensics, incident and breach management systems, and asset and vulnerability databases. The

---

<sup>5</sup> Seven Habits of Highly Effective Incident Response Teams, Forrester Research, Rick Holland, April 17, 2013  
Page | 12

strategic goal should be to provide all of the above capabilities as part of integrated platform that is used by the entire CIRC team.

Also in the *Seven Habits of Highly Effective Incident Response Teams* author Rick Holland of Forrester summed up the compelling business need for a mature incident response function emphasizing the positive business results of doing so, “In addition to protecting the firm’s IP, IR [incident response] is an opportunity to retain customer trust and safeguard the organization’s brand. Your customers (and the public at large) don’t expect your organization to be bulletproof; there is a growing sympathy for companies that fall victim to well-funded, highly skilled, organized cybercriminals. A well-coordinated, well-executed incident response that prioritizes transparent communication to customers and efforts to protect their identities and finances will actually enhance you organization’s brand.”<sup>6</sup>

## **RSA OFFERINGS THAT HELP TO ACCELERATE YOUR INCIDENT RESPONSE MATURITY JOURNEY**

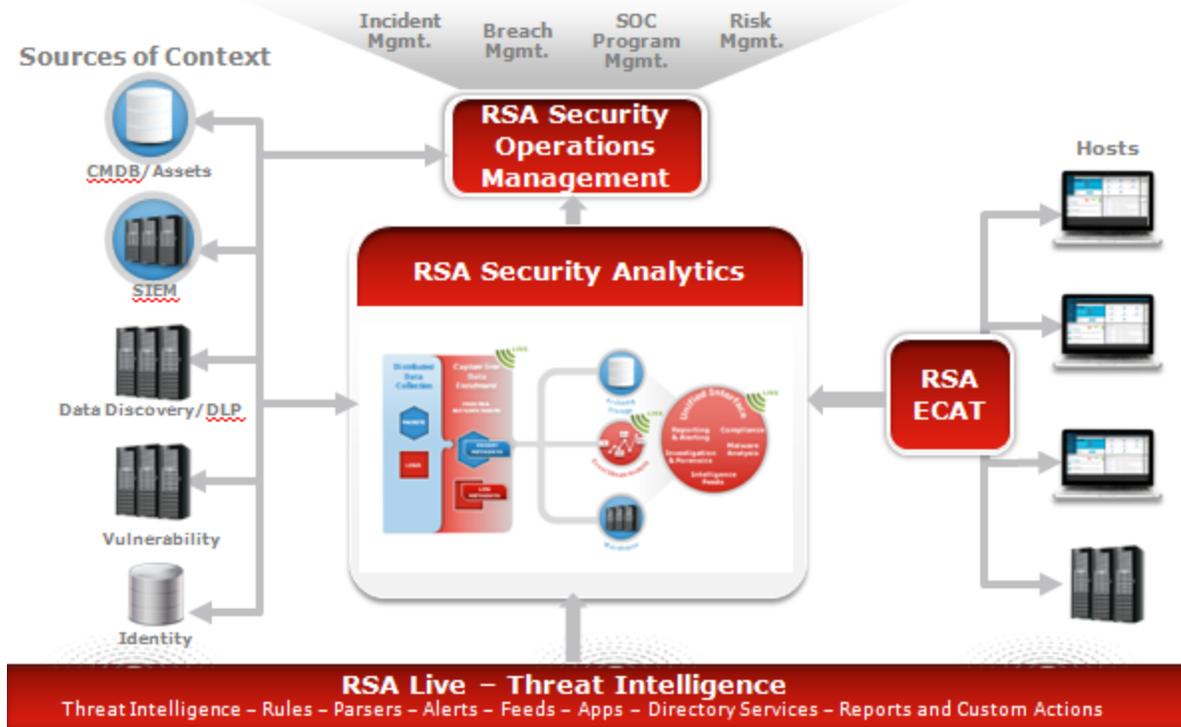
RSA can help you develop and grow your incident response team through focused and practical education, developed by incident responders, taught by incident responders, for incident responders. The [RSA Advanced Cyber Defense education series](#) is designed to provide a learning path for Tier/Level 1, 2, and 3 security analysts working in an incident response team. This series of courses provides role-based training on security principles, processes, and best practices using a variety of tools. This training series does not focus on the use of RSA products, but focuses on the skills needed by analysts to detect, investigate, and respond to security incidents and vulnerabilities. We at RSA certainly recognize there is a shortage of properly skilled incident response analysts, so instead of just going out on the market to find them, why don’t you grow some of your own?

RSA also provides a series of security consulting services that are specifically focused on delivering expertise to CIRC’s on breach readiness, response, and the design of security operations or incident response centers. The [RSA Advanced Cyber Defense Practice](#) (ACD Practice) is a global consultancy made up of incident responders and forensics experts that can help your organization improve its process maturity as well as provide advice on technology and skills gaps. The ACD Practice provides its services independent of the use of RSA products and focuses much of its efforts on the processes and expertise necessary to get the most out of the security technologies that are already in use by the organization.

RSA as a well known provider of security technologies also provides a broad set of modular, yet integrated detection, investigative, response, and management products that are used by incident response teams to improve their visibility, provide context, and better leverage their organization’s human expertise through various forms of automation. RSA collectively refers to this solution as the [RSA Critical Incident Response Solution](#). The technology portion of this solution combines the capabilities of [RSA Security Analytics](#), [RSA Live](#), [RSA ECAT](#), [RSA Security Operations Management](#), and [RSA Data Discovery](#) to provide incident response teams with the detection, investigative, response, and management automation they need to more effectively and efficiently do their jobs.

---

<sup>6</sup> Seven Habits of Highly Effective Incident Response Teams, Forrester Research, Rick Holland, April 17, 2013  
Page | 13



**THE RSA CRITICAL INCIDENT RESPONSE SOLUTION TECHNOLOGY**

**CONCLUSION**

Organizations’ IT infrastructures have become vastly more complex and harder to defend with the rapid evolution of the Internet, the Cloud, mobile computing, BYOD, Big Data, and the massive underlying technology diversity and ubiquitous usage. Add to this the level of sophistication, focus, and investment by the attacker community and you have a security market and defensive strategy that is need of change. However, there are internal forces arrayed against the security professional, as, for example, security budgets are not going up by much more than overall inflation. CISOs are being asked to address new threats with old budget levels that defend primarily against traditional threat vectors. And so much has been invested in the preventive security approach over the years that it is hard to bring forward the message that prevention will no longer be sufficient.

The clear answer for most organizations is to improve their detection, investigation, response, and management capabilities through the establishment of a centralized CIRC, while not depleting their worthwhile preventive controls. However, setting up, expanding, and maturing an incident response team cannot be done overnight even with infinite resources. Improved capability comes with continuous attention and investment over time. However, like with most challenging and uncertain journeys, the hardest step is often the first one. There is no time like the present to wade-in and get going. RSA is here to help you on your critical incident response maturity journey.

## AUTHOR BIOGRAPHY

Matthew Gardiner is a Senior Manager at RSA and is currently focused on the evolution of security management and monitoring solutions to better serve the detection, investigation, remediation, and management needs of security organizations. Before RSA Mr. Gardiner spent more than 10 years focused on identity & access management, Web access management, identity federation, cloud security, and IT compliance at Netegrity and CA Technologies. Previously he was President and a member of the board of trustees of the security industry non-profit, the Kantara Initiative. Mr. Gardiner has a BS in Electrical Engineering from the University of Pennsylvania and an SM in Management from MIT's Sloan School of Management. He can be followed on Twitter @jmatthewg1234

## CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, [contact](#) your local representative or authorized reseller—or visit us at [www.EMC.com](http://www.EMC.com).

Copyright © 2014 EMC Corporation. All Rights Reserved. H12651

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided “as is.” EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on [EMC.com](http://EMC.com).

EMC2, EMC, the EMC logo, and the RSA logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. VMware is a registered trademark of VMware, Inc. in the United States and/or other jurisdictions. All other trademarks used herein are the property of their respective owners.

