

# TRANSFORMING EXPECTATIONS FOR THREAT-INTELLIGENCE SHARING

August 2013

*Kathleen M. Moriarty*  
Global Lead Security Architect,  
Corporate Office of the CTO  
EMC Corporation

## KEY POINTS

Organizations today rely on information-sharing processes that are so manually intensive, duplicative, and inefficient that they cannot scale to meet critical computer network defense requirements of speed, agility, relevance, and accuracy. This gap ultimately translates into lost opportunities to avoid serious losses, improve security practices, prevent attacks, and predict threats.

The global security community should transform the methods, approaches, and expectations for the sharing of threat information by requiring what is shared to be 1) directed and actionable, and 2) aimed at providing a meaningful, and potentially automated corrective response.

Sharing information equally with everyone often results in information that's helpful to no one. Information-sharing processes are productive only if the intelligence disseminated is relevant to members' businesses and effective in helping them address threats or provide a proactive defense.

While actionable intelligence is always appreciated, automated defense in response to intelligence is preferred, especially by small- and medium-sized organizations that may lack the security resources to devise corrective measures on their own.

Certain industry consortia and working groups have integrated threat-intelligence gathering and response processes so tightly that the sharing of the underlying threat information actually is rendered unnecessary, because participants can leapfrog directly to corrective measures (e.g., updated block lists in browsers).

The security community achieves outsized results when it pools expertise and resources to analyze threats and develop solutions collaboratively. Expanded cooperation between tools/software vendors and Information Sharing and Analysis Centers (ISACs) is a promising direction to explore.

Exchanging security intelligence among other organizations has long been held up as key to achieving “situational awareness”—that is, understanding external threats clearly enough to assess their potential impact on an organization and formulate a response. Today, information sharing has assumed tremendous importance, given the rise of APTs and other targeted security attacks. With our hyper-connected networks, the prevalence of cloud, social media and mobile services, and the mounting complexity of most IT environments, advanced threats can hide in more places, spread faster, and cause more damage than ever before.

Information sharing is central to a new security approach called [Intelligence-Driven Security](#). In an Intelligence-Driven Security approach, organizations consume and process data from many diverse sources to assess in real time their exposures and risks, improve decision-making, prioritize security activities, and shorten the time needed to detect and respond to threats. Exchanging reliable threat intelligence with trusted external partners is pivotal to Intelligence-Driven Security.

Some organizations already exchange threat intelligence. Some participate in groups formed expressly to share threat information such as ISACs; others participate in passive ways, such as sharing harmful URLs with browser vendors to enhance block lists. Although threat-intelligence sharing yields value, it could and should yield far more. Overall, practices for sharing security information among organizations suffer from several shortcomings:

- **Shared data is difficult to act upon** – Threat intelligence often delivers low value because the information lacks sufficient detail and context, is unverified or is not well-matched to an organization’s business needs (i.e., does not apply to the organization’s vulnerabilities, system configurations, information assets or mission).
- **High levels of manual processing required** – Threat intelligence typically requires intensive processing by recipients (e.g., human sorting, normalization, cutting and pasting data between applications) to uncover what’s useful and make it actionable.
- **Redundant effort** – Each organization receiving threat data must often do its own processing and analysis of information, resulting in massive duplication of effort among recipients of security information.
- **Scarcity of skilled resources to analyze threats** – There are simply too few security experts available, considering the mountains of security data to be analyzed and the thousands of organizations needing their help.
- **Poor linkages to security controls** – Because of the lack of generally accepted standards, many threat-intelligence feeds are not easily integrated with security tools, creating delays in acting upon useful intelligence as controls await manual processing and activation by security experts.
- **Remediation addresses symptoms but not the cause** – Threat response may block URLs, change system configurations or take other corrective steps to prevent harm, but they do not address the root cause of the threat that creates recurrent vulnerabilities, such as understanding the tools, tactics and procedures used by adversaries or directly removing the threat.

The result of these deficiencies is that organizations today rely on information-sharing processes that are so manually intensive, duplicative, and inefficient that they cannot scale to meet critical computer network defense requirements of speed, agility, relevance and accuracy. This gap ultimately translates into lost opportunities to improve security practices, avoid serious losses, prevent attacks, and predict threats.

## WHAT ARE SHARING GROUPS?

Organizations that collect, process, and distribute threat intelligence as a service to their participants, members, and/or end-users.

Examples of sharing groups include:

- **Industry consortia** such as ISACS, APWG, and M3AAWG
- **Vendors** providing threat intelligence research and data feeds and/or commercial products and services integrating such feeds (e.g., security tools, browser providers)
- **Operators** such as Internet Service Providers (ISPs) and communications network providers

## THREAT INFORMATION MUST BE ACTIONABLE AND AUTOMATED

Addressing many of the current problems in information sharing will require the global security community to strive collectively for two goals:

1. Ensure that the dissemination of threat intelligence is relevant and actionable – This means our sharing efforts should be connected to a fundamental shared objective and identify an immediate and active security response focused on where it can have the greatest risk-mitigating effect.
2. Develop a speedy, sustainable, and scalable model to **automate reliable threat-information sharing among trusted parties and integrate response processes** to minimize or prevent damage.

For benchmarks on achieving these goals, we can examine a few of the sharing groups that have begun exchanging threat information in a directed, actionable way—with some even integrating with commercial-off-the-shelf (COTS) security tools for seamless threat remediation. Three notable examples are the groups exchanging email abuse information, anti-phishing information, and vendor threat-intelligence feeds.

### *Example 1: Preventing Email Abuse*

Large email service providers communicate via standards they developed to address email abuse problems (including spam). These providers address the abuse problem at the source, collaborating in the Messaging, Malware, Mobile Anti-Abuse Working Group (M3AAWG). Email operators determined what information was helpful to exchange in order to stop or mitigate email abuse directly with their peers: the operators of large email services. The operators have the ability to detect abuse and stop any abuse that originates through their services, providing effective defenses to these issues. These protections have broad benefits, reducing the overall threat in an automated way that does not burden users with having to take corrective steps themselves.

### *Example 2: Neutralizing Phishing Attacks*

One of the most notable and effective uses of information sharing is from the Anti-Phishing Working Group (APWG). The APWG coordinated with members affected by phishing (e.g., the financial industry) at the start of its work. It developed intelligence solutions that were later standardized to collect information into a centralized data warehouse. The APWG provides this clearinghouse of cybercrime data to its members, who then take actions to mitigate or stop threats. These actions include taking down the source of the phishing sites, which involves coordination with APWG vendor members and law enforcement. By targeting the sites that distribute email-based phishing attacks and the malware distribution servers (often included as links within phishing email attacks), APWG provides a focused and effective response that is directed at the source of the problem. Additionally, vendor members use the clearinghouse of cybercrime data to distribute preventive controls such as block lists that can be deployed to every desktop browser. Information is quickly distributed to where it can have the most effect while users remain unaware of the protections and the actual threat intelligence that have been deployed. This approach makes effective controls invisible and is a paragon of automated, dynamic remediation.

*Example 3: Integrating Security Controls with Intelligence Feeds*

COTS security software vendors and service providers' threat-intelligence feeds have typically focused on problem areas such as malware, network threats, web- and application-layer attacks, compromised identities, and other components of fraud. The APWG crosses the boundary into vendor/service provider threat-intelligence feeds, because commercial organizations often use APWG intelligence as one of their many data sources.

While the APWG combines many data sets for cybercrime in its clearinghouse, it's up to the participating COTS vendors, service providers, and threat-intelligence feed providers to provide an active response. They must deploy directed and actionable intelligence within their services and within the architectural frameworks of their products (e.g., integration of "live" intelligence or indicators of compromise into a security analytics platform).

This integrated approach is an early paradigm for how the practice of sharing threat information should be approached: IOCs need not be distributed as data in the clear; instead, they should be transformed on behalf of recipients into active response capabilities and mitigating controls. Many follow-on actions, such as blocking, black-holing, and black listing can be automated through tools controlled by security software vendors and service providers. Other remediation steps, such as the take-down of a command and control server or malware distribution site, can be undertaken by service providers for the benefit of all. Plus, the data required to implement corrective measures uses only small portions of the overall data set and can obviate having to disclose the larger underlying set of threat intelligence (e.g., IOCs), thus limiting the possibility of information leakage on threats or threat actors.

In order to provide actionable and automated threat-intelligence feeds, a number of COTS vendors and threat-intelligence service providers have sophisticated analytic centers with highly skilled experts utilizing multiple complex data sets. The analytic tools and formats are optimized within each of these environments to meet the changing needs of the business problems being solved by these teams. The analytic tools and data sets evolve continuously, with teams innovating to provide accurate threat-intelligence feeds and added value to customers. In some cases, data sets and formats will overlap; in other cases the business problems are sufficiently distinct.

## LESSONS LEARNED FROM INFORMATION-SHARING GROUPS

The sharing groups described above, in which security vendors, network operators, and industry consortia work together, are prime examples of how information-sharing activities can have a broad impact by generating either corrective action or actionable information that can be deployed as appropriate. From these examples we can derive several instructive insights:

- Sharing groups grow strong when members have shared business interests and thus similar business risks and security concerns. That's why sharing groups typically segment themselves by industry (e.g., financial services, state governments) or a business problem (e.g., reducing spam, preventing fraud, preventing denial of service attacks).

## WHEN DATA STANDARDS MATTER (OR NOT)

Information sharing standards provide a common interface or exchange mechanism to automate the transfer of information between two parties. In threat intelligence exchange, data format and protocol standards help ensure that the information packaged by the sender is “unpacked” and interpreted by the receiver as intended. Standards include policy details so information shared is protected and treated with the due care expected by the sender.

A sharing group may use different data formats and protocols to communicate with other sharing groups than it uses to share information internally. Or sharing groups may apply the same data standards to very different use cases, by either using certain portions of a standard or by selecting extensions to that standard. Security-related information that is exchanged less frequently or that varies over time can be handled using extensions to existing data formats, which may be standardized or private.

Interoperable data formats become important when exchanging data among different organizations, but interoperability is not necessarily the desired default state. Diversity in data formats allows for flexibility in product implementations. Security vendors use proprietary methods to communicate with deployed products and then use standards-based interfaces for interoperability between product implementations. Additionally, various de facto formats for data sharing have emerged within sharing groups with narrow fields of focus. To unify these disparate data formats, transformation mappings can be applied.

- ISPs, network operators, and other service providers who serve as gateways to large numbers of end users have developed effective, operationally focused information-sharing models by formalizing international standard data formats, such as the Incident Object Description Exchange Format (IODEF)<sup>1</sup> used by the APWG and the Abuse Reporting Format (ARF)<sup>2</sup> used by M3AAWG. Combining and correlating threat information provided by different sharing groups requires normalized data formats. Data standards become especially important for sharing among groups.
- Security service providers, industry consortia, and working groups have shown that threat- intelligence gathering and response processes can be coupled so closely for certain threat scenarios and use cases that information sharing is rendered unnecessary, because corrective measures can be taken automatically on behalf of participants and customers (e.g., block lists in browsers).
- While actionable intelligence is always appreciated, computer network defense that can be deployed automatically is preferred, especially by small- and medium-sized organizations that may lack the security resources to devise corrective measures on their own.
- The capability to deploy defenses without having to reveal underlying threat intelligence delivers security benefits while protecting the acquisition methods, integrity, and confidentiality of information sources.
- The security community achieves outsized results when it pools expertise and resources to work on complex security problems, obviating the need to solve problems in parallel and potentially arriving at solutions faster.

Perhaps the most important lesson to take away from successful information-sharing groups such as the APWG and M3AAWG is that sharing threat intelligence is not the end game. Information-sharing processes are productive only if the intelligence disseminated is relevant to members’ businesses and helps them address threats or provide a proactive, effective defense. Information that can be quickly distributed to where it can have the greatest effect—preferably while both general users and adversaries remain unaware of the protections deployed—is ideal. The APWG’s automated deployment of URL block lists in browsers is a classic example of this.

## SELECTIVE SHARING REDUCES THREAT-INFORMATION SPAM

Sharing information equally with everyone often results in information that’s helpful to no one. Threat-information sharing should be directed only to relevant parties and focused on a problem they care about.

### *Differentiate by Business Concerns and Mission Focus*

Differences in business interests and mission focus among sharing members will divide and dictate what should be shared. That’s why many of the most successful threat-information exchange groups are focused on a specific use case, mission objective or a business problem, such as distributed denial of service (DDoS) attacks, phishing attacks or tracking specific threat actors.

Whether threat intelligence is relevant or not is ultimately up to individual organizations to decide. To sort through the volumes of threat intelligence available to them, it’s imperative that organizations automate analysis of security information. Security tools

1 R. Danyliw, J. Meijer, Y. Demchenko; “The Incident Object Description Exchange Format” Internet Engineering Task Force (IETF) RFC 5070; December 2007

2 Y. Shafranovich, J. Levine, M. Kucherawy; “An Extensible Format for Email Feedback Reports” Internet Engineering Task Force (IETF) RFC 5965; August 2010

must be context-aware to assess the applicability of threat information to the organization. These assessments, which are often handled today by security personnel, will increasingly rely on the intersection of Big Data security analytics and asset-management platforms. In many large companies, different parts of the organization use different asset-management tools, making it challenging to get a unified, enterprise-wide picture of applicable risks and vulnerabilities. A single view of the organization's assets and configurations could be derived by integrating asset management platforms with security- and risk-analysis tools such as governance, risk, and compliance (GRC) systems. GRC platforms not only measure risks to assets, but they also monitor how those assets interact so mitigating controls can be adapted accordingly. Additionally, GRC tools can ingest threat intelligence, reprioritize risks and focus the organization or appropriate corrective action based on newly identified threats. Advanced GRC tools will integrate with security analytics tools, automating the evaluation and use of intelligence feeds providing broader situational awareness.

#### *Differentiate by Organizational Size*

Larger enterprises with sophisticated capabilities are typically interested in actionable intelligence that they can analyze and take action on themselves. Some use threat intelligence to help them understand and reduce the scope of threat actors they are facing. Small- and medium-sized organizations, on the other hand, often do not have the resources to participate in threat-information sharing groups or to pore through volumes of security data. Instead, smaller organizations prefer a turnkey approach in which risk remediation is handled for them, either by automated security tools or by service providers who host applications and data and manage security risks as part of service level agreements (SLAs).

Regardless of the size of the organization, GRC platforms must provide a business or mission context for the threat intelligence they collect. Risks and options should be assigned potential consequences and presented not as security or IT decisions but as business-level decisions.

## CONCLUSION

Gathering external threat intelligence is essential to assessing an organization's real risks. As part of an Intelligence-Driven Security program, threat information can help organizations prioritize security activities and shorten the time needed to detect and respond to potential threats.

Many organizations participating in threat-intelligence-sharing programs suffer from TMI (too much information), while others struggle to use threat intelligence that's neither relevant nor actionable to their business/mission objectives. In disseminating threat information, information-sharing groups must keep in mind that intelligence itself is not the goal; remediating risks and neutralizing threats is. To this end, information-sharing programs must do the following:

1. Make the dissemination of threat intelligence directed, relevant, and actionable – This means our sharing efforts should identify an immediate and active security response focused on where it can have the greatest effect.
2. Develop a speedy, sustainable, and scalable model to automate information sharing and threat response.

Simultaneously, we must improve information-sharing and analysis processes so that fewer security experts are needed to address problems. One way of achieving this is to pool resources and work on problem resolution collaboratively. A promising avenue to explore is enhanced cooperation between threat analysis centers, such as ISACs, communications service providers and software and security tool vendors.

When external threat intelligence is actionable, relevant and triggers a corrective response, organizations can expand situational awareness and improve security not just for themselves but also for their information-sharing partners.

---

*The author wishes to acknowledge the following EMC and RSA colleagues for their contributions, edits, and validation of trends and positive direction: David Black, Tim Belcher, Rear Adm. Mike Brown (Ret.), Seth Geftic, Brian Girardi, William Gragido, Chris Harrington, Erik Mogus, Alok Ojha, Paul Stoecker, Eddie Schwartz, John Swift, Steve Todd, and Peter Tran.*

## ABOUT RSA

RSA, The Security Division of EMC, is the premier provider of security, risk and compliance management solutions for business acceleration. RSA helps the world's leading organizations solve their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, encryption & key management, SIEM, data loss prevention, continuous network monitoring, and fraud protection with industry leading GRC capabilities and robust consulting services, RSA brings visibility and trust to millions of user identities, the transactions that they perform and the data that is generated. For more information, please visit [www.RSA.com](http://www.RSA.com) and [www.EMC.com](http://www.EMC.com).

EMC<sup>2</sup>, EMC, the EMC logo, RSA and the RSA logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other products or services mentioned are trademarks of their respective companies.

© Copyright 2013 EMC Corporation. All rights reserved.

[www.rsa.com](http://www.rsa.com)

223649-H12175-TIS-BRF-0213