Collaborative Defense
Cyber Incident Planning and Response

The Roles of Legal Counsels and Communications Executives at Sophisticated Organizations

Field Research from ACSC Collaborative Defense Report
January 20, 2020

ADVANCED CYBER SECURITY CENTER
COLLABORATIVE DEFENSE • TRUSTED NETWORKS

ACKNOWLEDGEMENTS

Thank you to all the ACSC member organizations for their engagement and support, which made this research and report possible. Our gratitude to the following individuals, whose interviews provided the material for this report:

Legal Counsels
Launch Roundtable
Foley Hoag
July 30, 2019

Michele Gerroir, Blue Cross Blue Shield of MA
Jim Gwinn, Dell
Joffrey Hill, National Grid
Daniel Hoag, MITRE
Andrew Karberg, University of Massachusetts
Raisa Litmanovich, Rapid7
Amy Mugherini State Street
Anthony O'Neill, Commonwealth of Massachusetts
Dawn Rogers, Veracode
Christopher Sloan, Liberty Mutual*
David Suski, MIT Lincoln Laboratory
Shana York, Mimecast
Colin Zick, Foley Hoag LLP*
Stephanie Zierten, Federal Reserve Bank of Boston
**Chairs*

Communications Executives
Launch Roundtable
Rapid7
September 6, 2019

Jen Ellis, Rapid7
Tim Hamilton, Mimecast North America
John Hoey, UMass Dartmouth
Jessica Lavery, Veracode
Karen Lilla, Liberty Mutual
Ryan Murphy, Carbon Black
Lisa Natalicchio, State Street
Alison Walsh, Mimecast
Cheryl Wadsworth, Rapid7
Lucy Warsh, Federal Reserve Bank of Boston

ABOUT THE AUTHOR

Interviews were conducted and this report was written by William Guenther, with assistance from Emily Walt and Kathryn Plazak.

William Guenther is the Executive Chairman and founder of the ACSC, and also the Chairman, CEO and Founder of Mass Insight Global Partnerships.

Emily Walt is the ACSC Director of Member Engagement and Communications.

Kathryn Plazak is the President of Plazak Associates and a consultant to ACSC.

The Advanced Cyber Security Center (ACSC) is the region's only non-profit, member-driven organization committed to strengthening member cybersecurity defenses and preparing the region's response to large scale cyber threats. The ACSC was established in 2012, as a 501(c)3 organization and was the model for Information Sharing and Analysis Organizations (ISAOs) when Presidential Executive Order 13691 was implemented in 2015. Currently the ACSC has 27 members representing the financial services, healthcare, technology and utilities industries, along with leading universities and the Commonwealth of Massachusetts.

The ACSC is located at The MITRE Corporation, 202 Burlington Rd, Bedford, MA.

TABLE OF CONTENTS

OBJECTIVES AND METHODOLOGY

The objective of this effective practice field research was to examine the evolving role of legal counsels and communication executives as they work with security executive colleagues to prepare for and respond to major cyber incidents. The findings are based on 14 interviews with ACSC member legal counsels and nine interviews with communications executives (see Acknowledgements for list).

This is the third in a series of reports on Collaborative Defense practice defined as collaboration across corporate functions and between organizations and the public and private sectors. The first, “Collaborative Cyber Defense: Barriers and Best Practices for Strengthening Cyber Defense by Collaborating Within and Across Organizations,” and second, “Leveraging Board Governance for Cybersecurity: The CISO/CIO Perspective,” can be found on the ACSC website.

OVERVIEW

A New Challenge, New Disciplines, New Cyber Roles

As with the senior executive CISO role, **dedicated counsels for cybersecurity and senior communications staff deeply engaged with cyber defense are new corporate developments in the last decade.** Many organizations have only recently assigned significant cybersecurity legal responsibilities to one member of the counsel team, and have brought communications staff into incident planning and response as full partners.

Counsels coming from other disciplines and communications executives are required to become more and more knowledgeable about cybersecurity and keep up with issues and trends that affect their important contribution to cyber preparedness. This is made more challenging in that counsels and communications executives report that **there is no single comprehensive source of current information that can inform their work,** and the often-used NIST framework offers little guidance in this regard.

Cyber incident planning and response has been in some cases organized as a subset of existing emergency preparedness groups, which has led to additional challenges, especially the need to differentiate the distinct procedures, systems, and language for cyber preparedness from more traditional emergency practices.

A Deep Engagement with Incident Planning and Response – and Participation in Regular Simulations

It is no surprise therefore that the **role for both legal counsels and communications executives is also evolving** in the preparation for and response to the number and scale of cyber incidents their organizations face.

Increasingly, both legal counsel and communication executives are included in cross-functional, integrated cyber response teams formed to advance cyber resiliency. Both legal and communications staff are active participants in incident planning, overlaying their requirements on plans developed by security staff.

One counsel, however, emphasized the important adage:

> ***“Plans are only as good as the practice.”***

Most often both functions take part in at least an annual interdisciplinary simulation exercise run by their organizations. The most sophisticated organizations run simulations engaging senior executives including legal and communications on a quarterly basis. Sometimes even corporate board members participate on an annual basis.

Integrated Cross-Functional Response Teams Usually Include

- CISOs
- Security/Tech/Ops
- Business Lead
- Legal Counsel
- Communications
- Compliance

Triggers with Metrics Set the Rules of Functional Engagement in Cyber Mature Organizations

Sophisticated incident plans include specific triggers for when legal and communications staff and more senior executives are brought in, depending on the seriousness of an incident, although CISO judgement remains a significant factor in most organizations. Common triggers tied to severity levels of 1-4 can include when customers are affected for a period of time, when an incident affects key operations, or when a law or policy is violated.

Outside Experts are Commonly Used, but Rarely Engaged with Planning on a Regular Basis in Large Organizations

Both legal and communications disciplines use outside experts including outside counsel, crisis communications and forensic consultants to varying degrees, depending on the depth of internal resources in these areas. More often, **organizations only engage outside resources in exceptional circumstances** and rarely in the training exercises and simulations that they run. Not surprisingly, outside experts are more often used by smaller and mid-size organizations.

Building Trusted Internal and External Relationships Before They are Needed is Critical

To be effective in their respective roles, both legal and communications staff need to **establish strong working relationships with their counterparts throughout the organization, before a crisis occurs.** Both report the importance of “soft skills” for their success in building these trusted relationships, in order to become embedded members of the security team and to engage with government regulators. It is also to their advantage to develop these trusted networks, externally as well as internally, to enhance their skills and knowledge.

LEGAL COUNSELS

Privacy and Security Counsels are Becoming More Important and Active Partners with Security Teams as Cyber Risks Increase in Number and Scale

The increasing rate and complexity of cyber incidents is driving the need for legal counsels to be experts on legal and regulatory requirements governing these incidents, and to partner closely with their organization's security team. While in some organizations legal counsels are still "on the periphery" of incident planning and response, for most organizations their legal teams have become key partners.

CISOs and the security teams drive the development of procedures and plans for incident response; **legal counsel reviews and advises on compliance and has an ongoing and close collaboration with the security team to ensure that plans and practice comply with all applicable laws and regulations.**

> *"Legal's role is to help the Security Team achieve their goals, and think through their processes within the context of legal and compliance requirements."*

In addition to helping to prepare their own organizations for cyber incidents, **legal counsel are key to managing risk in contracts, especially for the supply chain.** Most are deeply engaged in reviewing vendor contracts for privacy and security requirements, presence of cyber insurance, etc. Some states, such as New York, require that financial service organizations certify for vendor data privacy and security standards.

Outside counsel can play an important role in developing a compliant cyber incident plan and response. Even in larger organizations, outside counsel can be a valuable source of information given the myriad of state, federal and global laws and requirements – often a challenge for in-house counsel to keep up with. Some use outside counsel to reinforce or independently assess their plans, and present to their CEO or boards, helping to assure CEO and board buy-in. Many organizations report having outside counsel on retainer, although fewer use them during incidents except in extreme cases. **When to engage outside counsel should be articulated in the cyber incident response plan.**

Attorney-client privilege and work-product protections can be important elements of investigations into cyber incidents. Counsels report varying success in assuring their colleagues regularly assign privilege to communications that should have the protection.

This relatively new cybersecurity role for legal counsels comes with **a number of challenges** and within increasingly complex circumstances, including:

- Global, U.S. and multiple state privacy and security **requirements vary significantly**, and new state legislation and regulations are constantly being proposed.
- There is **no single source of current information on applicable laws and regulations,** which come from states, federal government, and global entities. (See appendix for some sources of information.)
- **Industry and organizational standards** may well exceed legal and regulatory requirements.
- **Trusted networks** (internal and external) can be an important resource for legal counsels, but there **appear to be few of these** in the region for privacy and security developments and none specifically for incident planning and response practice.
- While most organizations employ the **NIST framework, it contains little guidance on the role of legal counsel** in incident response.
- **For outside counsel,** a challenge is to have a defined role and engage a client organization's attention/time before a crisis.

Preparing for Incidents: Counsels set the “Legal Guardrails”

CISOs and their security teams drive the development of cyber crisis plans, but legal counsels set the “legal guardrails” to ensure compliance with laws and regulations. Most organizations have created a cross-functional team to develop and regularly review cyber preparedness that includes security, legal, communications, government relations, business heads, and others. Having legal counsel deeply integrated in this team is essential. Each member has clear lines of authority to make decisions, and the teams meet regularly.

> *In our company “legal touches base weekly with security and communications, especially on changes in regulations, laws, and particular threats.”*

To be successful in this role, it is **important that legal counsels develop cross-functional relationships with all departments** critical to incident response. Counsel’s role in preparing for cyber incidents includes:

- **Help staff think through the escalation triggers** within the context of existing laws and regulations. (Note that while a hierarchy of notifications is generally defined – and in the most sophisticated cases, with 1-4 severity levels and specific triggers – CISOs retain significant responsibility making the call as to when/how to escalate.)
- **Review policies and plans for compliance;** regularly review and ensure updates to the plan as laws and regulations change.
- Ensure that **requirements driven by contracts are included in the plans,** especially where government contracts are an issue.
- **Ensure that federal and state officials/other external contacts are clearly listed** in the plan and relationships developed and sustained on a regular basis (a challenge with the turnover in government staff in some areas).
- **Participate in simulations.** While not yet universally involved in an organization’s annual simulation exercises, legal counsels are most often part of the cross-functional team that participates, an essential element in practicing response and coordinating roles during an incident.
- Particularly challenging for organizations with national and global offices, **ensure there is consistency across units** in their planning and practice and coordination of incident responses.

> *“Legal Counsels are not just part of the plan, they are part of the practice.”*

During Incidents: Timing of Legal Engagement is Key

Even with the best cyber crisis plans, the timing of when to involve other players (internal and external) beyond the security staff is critical. Having defined severity levels will trigger the engagement of key executives, including legal counsel, communications, external regulators, etc. For most organizations**, incidents that affect key strategies or operations, or that violate law or policy trigger the involvement of legal counsel.**

Legal counsel's role during an incident includes:

- **Ensure that everyone follows the plan and that policies are understood and followed.**
- Assure that **appropriate privileged communications are in place**. Those public sector organizations subject to Public Records requirements have an additional concern about what they document. Organizations disclosing incidents to law enforcement or regulators also need to consider if and when such disclosures could be subject to public disclosure.
- **With communications executives, make judgements about external communications** - release too much information and you expose yourself; too little and you compromise transparency. Legal is a key funnel for the timing and consistent messaging in communications.
- Weigh in on **when to pull in outside counsels**.
- Determine **whether and when to bring in government officials/regulators** (whereas early is usually advisable, but not useful until the basic facts are established).
- **Consider insurance implications** – provide notice to insurer, determine if the incident should be covered, and if so, manage the communications and documentation of same during a material incident.

Challenges during an incident include:

- It's easy to over or under-react. **Make sure people follow the plan** and don't get ahead of themselves and make premature notifications.
- **Different departments often have different constituencies** with different interests and agendas.
- Timing of notifications can be tricky.
- **Enforcing privilege and communications guidelines.** As one counsel noted, you need to "manage well-meaning individuals discussing information in unprotected emails."

Incident Planning and Response: The Government's Role

To best leverage government's regulatory and compliance roles, it is **critical to build relationships with key government contacts early – well before you need them in a crisis.** Arrange regular meetings. Make them trusted partners before an incident occurs, then help them do their jobs during an incident.

On threat sharing and collaboration during incidents, however, there is continuing skepticism among legal counsels about the value of government's role. Most see government as a source of onerous reporting requirements rather than assistance, and some are not surprisingly leery of providing more information than is required for fear of having their organizations investigated. This issue is exacerbated by what some perceive as a lack of commitment to privileged communications and privacy. In some cases, government has been found not to have adequately protected information shared.

Relationships with government are also complicated by high staff turnover among some branches and agencies.

> *"Understand the regulator's job and help them do it."*

> *"I have seen actionable information when I was in government, but the government does not share that actionable information with the private sector."*

COMMUNICATIONS EXECUTIVES

Communications Cyber Response Teams Can Include

- Internal/Employee Communications
- External Communications/PR Social Media/Digital
- CMO
- Business Unit Communications
- Crisis Communications/PR Agency

The Role of Communications Teams is Growing in Cyber Preparedness

Communications executives are increasingly expected to be an active partner with their security teams in preparing for and responding to cyber incidents. As with legal counsels, this **requires that they become more knowledgeable about cybersecurity in general, and incident preparation and response specifically.** To fully engage, interdisciplinary communications teams are often formed to fill specific roles in helping to develop a response plan, and also to act during an incident.

Particular challenges in this new, expanded role for communications executives include:

- **Staying abreast of cyber issues and trends,** especially with few professional sources of information.
- **Internal reporting structures** often involve dual reporting and multiple dotted lines across the organization, which sometimes present multiple or even dueling priorities to address.
- In a multi-channel, social media world, **balancing consistent messages and the sequencing of communications across multiple constituencies** including employees, customers and media.
- In national and global organizations, especially those with local communications staff, **managing across units, geographies and time zones.**

Few Good Information Sources to Stay Up to Date

Staying current on cybersecurity issues and trends from a communications perspective can be a special challenge, as there are **few regular professional sources of this information and limited professional guidance.** Most organizations use the **NIST framework, but this offers little guidance on the role of communications.** Professional associations like PRSA and IABC don’t provide much focus. Some staff use daily news services from the WSJ, trade publications and blogs for background, but it is time-consuming to cull through sources. Geo-political tensions continue to manifest in cyberspace, further accelerating the need (and cadence) for understanding.

Outside PR firms can be helpful in tracking developments, although most organizations use outside firms for cyber crisis communicators and during the most serious incidents only. (See Appendix for sources of information for communications staff.)

Trusted peer networks would ordinarily be valuable but are typically more tech-focused, so not as helpful to the communications professionals. Peer networks can also be complicated by a reluctance to share sensitive information.

Preparing for Incidents: Planning for Multiple Scenarios

The communications team is increasingly an integral part of a multi-disciplinary, cross-organizational team led by the organization's CISO. **Communications staff, in conjunction with legal and security staff in particular, develop plans to respond to multiple scenarios** including when, how and who should respond during incidents.

To be an effective member of the cyber preparedness team, communications staff need to **establish strong relationships with counterparts** throughout their organization.

> *"Build relationships, establish roles, have templates ready before an incident - and test practice."*

The communications staff's role in incident preparation includes:

- **Ensure that the appropriate communications staff are identified** and part of the team, and that communications decision-makers are clearly designated. It's a particular challenge for large and geographically dispersed organizations to clarify roles with local staff.
- Ensure that there are **points of contact** for each function with authority on communications issues.
- Identify **spokespersons for various scenarios.**
- Review plans/playbooks to **ensure that communications considerations are appropriately woven throughout,** and that triggers are established as to when to engage and when to escalate. (Note that while triggers are defined in a plan, it is in many cases the CISO's call when to trigger next steps.)
- **Create templates and tools ahead of time,** such press releases, but with enough flexibility to adapt to a particular incident.
- **Participate in organizational simulation exercises** to practice and develop "muscle memory" for activities during an incident.
- **Select the appropriate communications platforms** to use throughout the plan (i.e. internal communications tools such as intranet and texting, and external tools such as use of website, Twitter), and plan for alternatives when/if these tools are made inaccessible due to the incident.

> "Better to be right than be fast." Communicate, but not more than you know. Manage external messaging, including using websites and social media, through the sequencing required for each incident.
>
> - First, general knowledge of an incident and that we're dealing with it - more information to follow.
> - Second, more comprehensive, with details
> - Third, corporate spokesperson provides briefing to specific audiences.

During an Incident: Delivering Appropriate Messages with Verifiable Information on a Timely Basis

CISOs and the security teams are the authoritative source of technical information about an incident. Communications staff, when pulled into an incident, **play a key role in "thinking like a journalist" and making sure that all facts are verifiable** and that the organization doesn't get ahead of itself in communicating either internally or externally.

Key communications considerations during an incident:

- **Don't act prematurely** – know the facts before you act.
- **Coordinate with legal counsel** to review language.
- **Use social media in multiple ways,** to distribute messages and also to assess the need for a response. If there's little chatter, don't increase the conversation.

Some of the most frequently-cited communications challenges during an incident include:

- Getting **verifiable information on a timely basis;** finding the single point of truth.
- Lack of **clarity over ownership** of specific aspects of the response.
- Resisting communicating before you know the facts.
- **Managing social media:** Projecting the message without fueling the fire. **Avoiding decisions simply based on the level of noise.**
- **Failure of technology tools** (i.e. internet down)
- **Ensuring consistent messaging** across large and disbursed organizations

During an incident: "If there is a little chatter, don't increase the conversation."

Communications Tools Often Used in Incidents

- Everbridge
- Slack
- Zoom (to reduce "noise" on Slack)
- Open conference call bridges
- Intranet and customer portals
- SMS messaging
- Social and digital media (Twitter, LinkedIn, website, blogs to communicate and monitor activity)

RESOURCES

Legal

Law360: www.law360.com (subscription required)

The CyberWire: https://thecyberwire.com/

Lexology: https://www.lexology.com/

Center on Privacy & Technology at Georgetown Law Center:
https://www.law.georgetown.edu/privacy-technology-center/

National Association of State CIOs: https://www.nascio.org/

National Association of State AGs: https://www.naag.org/

Association of Corporate Counsels: https://www.acc.com/chapters-networks/chapters/northeast

ABA - National Security Division: https://www.americanbar.org/groups/public_interest/law_national_security/

NE Corporate Counsel Association: http://www.necca.com/

IT Law Association: https://www.itechlaw.org/

IAPP: https://iapp.org

Infragard: https://www.infragard.org/

FS-ISAC: https://www.fsisac.com/

Communications

PRSA: www.prsa.org

IABC: www.iabc.com