sedgwick

Sean Wood

Katherine Goodyear

Spotlight

Sedgwick's brand protection spotlight features insight and perspective from our strategic partners across industries on safety issues that have potential to influence a company's view on product-related crises.

In this edition, we are joined by Sean Wood, Executive Vice President and Katherine Goodyear, Account Director at Weber Shandwick for an overview of cybersecurity communications. We explore what companies should do to plan for an incident, and the practical steps they should take to best minimize the impact, protect and enhance brand reputation should one occur.

—

When a cyber-attack strikes: protecting and repairing brand reputation

Cybersecurity incidents are among the most serious business and reputational threats facing companies and can quickly erode trust by key stakeholders — from customers to employees to the general public. On top of that, they're difficult to resolve, costly and fast-growing.

Cybercrime is expected to cost approximately $6 trillion USD in damages globally in 2021, up twofold from 2015 — and ransomware attacks shot up 151% in the first half of 2021, compared to full-year 2020.

The consistent increase in these incidents, their sophistication and their potential operational and financial impact underscores how important it is for companies in all industries to be prepared.

In fact, a recent global survey conducted by KRC Research and Weber Shandwick of executives in 12 countries revealed that cybersecurity and data privacy are the top two concerns for executives when making important business decisions.

Getting ahead by planning ahead

While people understand cybersecurity incidents happen, they often judge companies and organizations on how they respond — and hold them accountable when information is exposed or misused. For this reason, the number one company priority should be getting a pre-incident plan in place to allow the business to respond quickly to an attack.

Not only is this planning the right thing to do to protect sensitive personal and commercial information and brand reputation, but customers, insurers and the government are underscoring the importance of strengthening incident response plans. Recently, United States President Joe Biden held a meeting where he described cybersecurity as a "core national security challenge," and called for the private sector to bolster the nation's cybersecurity in partnership and individually, with an emphasis on solving a cybersecurity skills shortage. Following Counter-Ransomware Initiative meetings held in October by the White House National Security Council, over 30 countries and the European Union issued a joint statement of cooperation to improve national resilience, counter illicit finance, disrupt ransomware criminals, and utilize diplomacy as a tool to counter ransomware.

In this instance, planning means:

- **Developing or updating an incident response plan.** Covering both operational and communications responses, these plans should be integrated and outline who needs to be involved, roles and responsibilities, risk levels and thresholds and indicate a process for swift communications to impacted stakeholders.

- **Establishing scenario planning for potential risks and incidents.** The scenario plan should include situation-specific considerations and guidance, as well as template stakeholder messaging that can be quickly updated with the facts of the actual situation should an incident arise.
- **Testing the plan.** Conducting realistic simulation drills is an important part of the planning and preparation process to test the organization's ability to function according to the plan and protocols. It will also identify gaps in processes that need to be patched before a real event occurs.
- **Investing in advance.** Some organizations may feel they are unable to invest in advance to have a contingency call center or other solutions in place, but it is the best way to avoid being unprepared. This investment may include putting in place a loss notification/breach response call center. It also may involve a secondary, separately hosted information hub or microsite, which can be turned on quickly to communicate to stakeholders via alternate channels in the event you lose access to your systems.

Now, when an incident occurs, your company or organization is better prepared to manage the situation, to activate the plan in place and focus on mitigating any risk.

Implementing the plan

When an incident happens, the company should immediately move into activating its regularly updated incident response plan. Be transparent, but don't get ahead of the facts. Data forensics often take time, so it is important to communicate only confirmed facts and acknowledge that the situation is fluid and may change.

To minimize impact, protect and potentially enhance brand reputation, there are several considerations to keep in mind:

Perception:

Often, perception is that a company or organization is accountable even if they're not responsible for breached data. Stakeholders can and will forgive you for security lapses, bad luck or even both. But attempting to deflect the blame may backfire. Those affected by the mishap see it simply: They trusted you with their information and you lost it.

Control:

You (the company or organization) may not have control of disclosure timing. There are many factors that may accelerate your response. For example, countries and U.S. states have different disclosure requirements. The media cycle or social media commentary may also force it. Hackers leak confidential information to the web, which is then picked up by cybersecurity reporters and bloggers. Staff can also inadvertently leak sensitive information, adding to the problem.

Obligation:

Companies and organizations may have contractual obligations to disclose the incident. Increasingly, contracts with vendors and partners include clauses requiring companies to disclose a breach, regardless of regulatory requirements. If the company is public, there may be material impact and related considerations that need to be factored in, on top of regulatory disclosures.

Communication:

Not every incident demands proactive communication of the whole situation to all audiences. The decision to be proactive or reactive and with which audiences is nuanced and not a one-size-fits-all model. Even if there are not contractual or regulatory requirements, companies may have an ethical requirement to disclose — often driven by the scope of the breach and the likelihood for it to become public. *(Pro tip: it's always better for your stakeholders to hear from you versus finding out for the first time in the media. Doing so shows that you take the protection of their information seriously.)*

Values:

Always ground business response in business values. Who do you stand for as a company and what would your stakeholders expect from you? See the situation through their eyes and respond accordingly.

The alarming rise in cybersecurity incidents over the past year, as well as the number of well-publicized breaches, underscores that there has never been a more important time to prepare. With more organizations and companies pursuing a hybrid model of work, the risk of a data breach only continues to increase. Threat actors will see an opportunity with a remote workforce — and we should expect that they will continue to evolve and adapt their operations to the new normal.

Prioritizing cybersecurity planning now will help to ensure your organization is prepared in the event an incident arises -- because it's not a matter of "if" but a matter of "when" a cyberattack will occur.

About our guest authors

Sean Wood

Sean Wood is an Executive Vice President in Weber Shandwick's Global Crisis & Issues practice. He has helped clients across industries safeguard their reputations in high-stakes situations for more than 25 years. Sean brings a corporate and brand reputation lens to crisis and issues management to help business leaders address complex situations with integrated strategies to mitigate risk.

Sean has helped clients prepare for, manage and recover from a wide array of complex, sensitive issues and crises, including cybersecurity incidents, regulatory issues, litigation, public health emergencies and other disasters, recalls and other product safety issues, and management and business transformations. He oversees a specialty area focused on cybersecurity communications and has guided clients in planning, training for and navigating live incidents – from ransomware-driven system outages to phishing campaigns to third-party breaches.

Sean graduated with a B.A. in Soviet Studies from the University of Pennsylvania.

Katherine Goodyear

Katherine Goodyear is a Director in Weber Shandwick's Crisis & Issues Practice in New York City. Over the past five-and-a-half years, Katherine has counseled clients through their most complex and sensitive issues to protect their reputation. She provides a full range of crisis communications support, including crisis planning and preparedness, as well as day-to-day issues mitigation, 24/7 support in live situations and reputation recovery support post crisis. Katherine has helped clients across a range of industries navigate cybersecurity incidents, including third-party data breaches, phishing campaigns, malware and ransomware attacks. Katherine also leads crisis simulation drills using Weber Shandwick's award-winning interactive crisis simulation platform, Firebell.

In 2019, Katherine was named a "Rising Star" by PRNews. She graduated magna cum laude from Carleton College with a B.A. in sociology/anthropology and European Studies.

About spotlight

Brand and reputation are the most valuable and vulnerable assets a business has. Brands embody and encapsulate everything a business does, and its customers expect. Nothing says more about a company's commitment to its customers than its efforts to uphold promises of safety, quality and service. However, too often, recall and remediation management is treated as a low priority, only to be applied – or even discussed – when a product needs to be withdrawn from the market. We seek to change that.

Sedgwick's brand protection spotlight is our way of sharing perspectives from our strategic partners – lawyers, insurers, risk managers and crisis communications experts across industries – on product safety issues that have the potential to influence a company's view on in-market incidents and crisis management. In some cases, the connection is obvious but the perspective is new. In others, we will raise questions that you may have never considered in the context of recall and remediation management. That's our intent.

—

To learn more about our recall, remediation and retention solutions, contact:

P. 888.732.3901 **E.** brand.protection@sedgwick.com

To learn more about our brand protection solutions, visit **SEDGWICK.COM/BRANDPROTECTION**