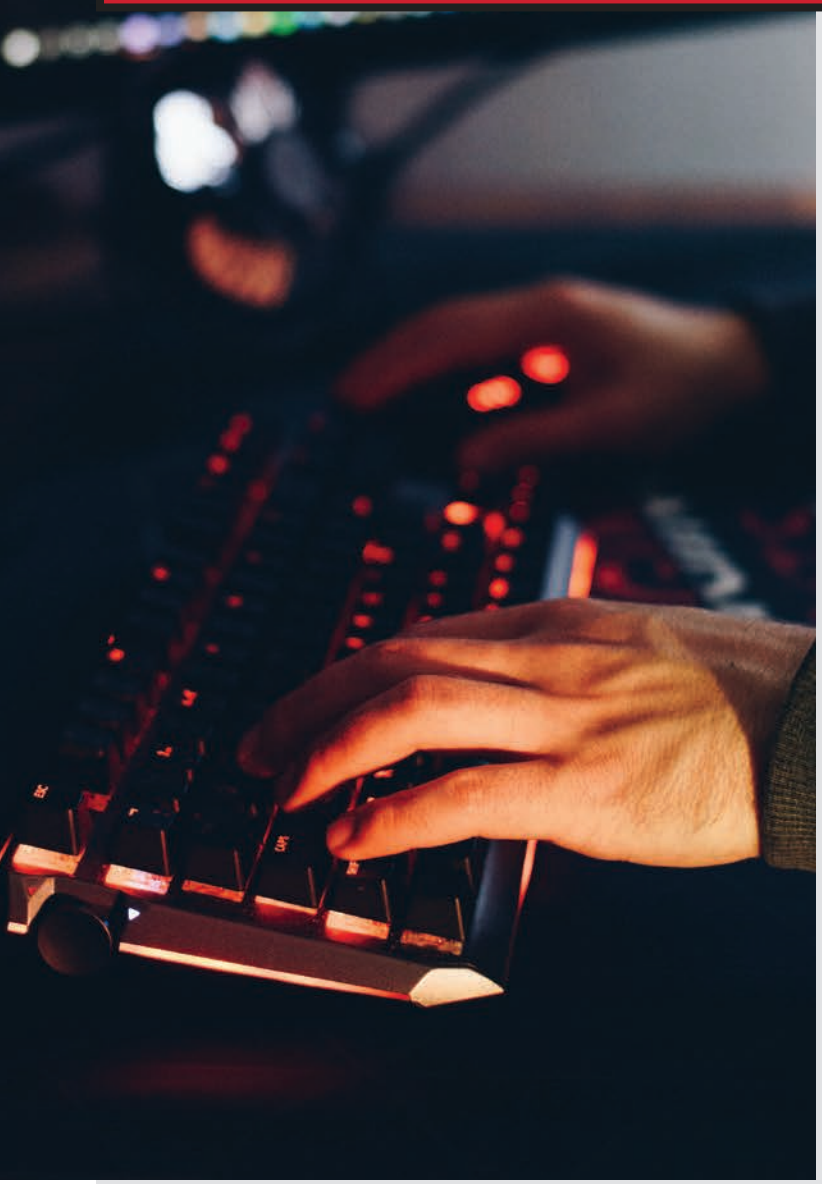
NETSPI

HOW TO COMMUNICATE A CYBERSECURITY BREACH



800 Washington Ave. N.
Suite 670
Minneapolis, MN 55401

E : info@netspi.com
W: www.netspi.com
P : 612.465.8880

NETSPI™

Visit the NetSPI resources webpage or skim our blogs and you'll quickly notice that most of our content is made for those in an IT or cybersecurity role – from CTOs to infosec managers to penetration testers. However, cybersecurity is everyone's business, even more so during Cyber Security Awareness Month.

It's no surprise that for many organizations, cybersecurity breaches are a "high reputational risk" crisis scenario. It's important to remember that, given the increasing sophistication of attacks, cybersecurity breaches today are inevitable. Organizations must get proactive about their crisis management policies and procedures. And it's critical that the plan is communicated and adopted beyond the security and IT teams.

Navigating a breach scenario is no simple task. A quick visit to the National Conference of State Legislatures website reiterates the complexity of state-by-state breach disclosure laws. Each legislature includes varying provisions regarding who must comply, how personally identifiable information (PII) is defined, what constitutes a breach, and more.

To help, if you happen to find yourself in a position where you must disclose a breach, we've outlined 5 communications best practices to consider:

1 Ensure you have the right people on your crisis management team.

Establish a crisis management team with leaders spanning the C-Suite, privacy, IT, sales, customer success, people operations/HR, finance, marketing, and engineering. All departments across the organization have a role to play.

2 Spend time on logistical items now, so that you can focus on remediation later.

Proactively work with legal and finance teams to understand which regulatory bodies, government entities, and insurance agencies to notify. Gather key contact information so that it is at the ready. Better to focus on the breach impact and mitigation than to spend time looking for your cyber insurer's phone number.

3 Be the first and primary source of information.

Ensure your organization is the go-to resource for the facts – before news articles, social media discussions, word of mouth. Ensure you are continuously providing updates in real-time. It may be valuable to create a webpage dedicated to event updates.

4 Alignment with the IT and security teams is vital.

Meet with the assigned technical team to understand the breach, its impact, and the actions being taken by your organization to remediate. Questions to ask include:

A. Is the breach contained?

B. What's the scope of this incident?

C. Does it violate any regulatory standards (PCI, HIPAA, GDPR, CCPA)?

D. Who is affected?

E. What did the attack campaign look like—and are the attackers still present?

F. What is the estimated timeline for mitigation?

G. What is our legal obligation for breach notification?

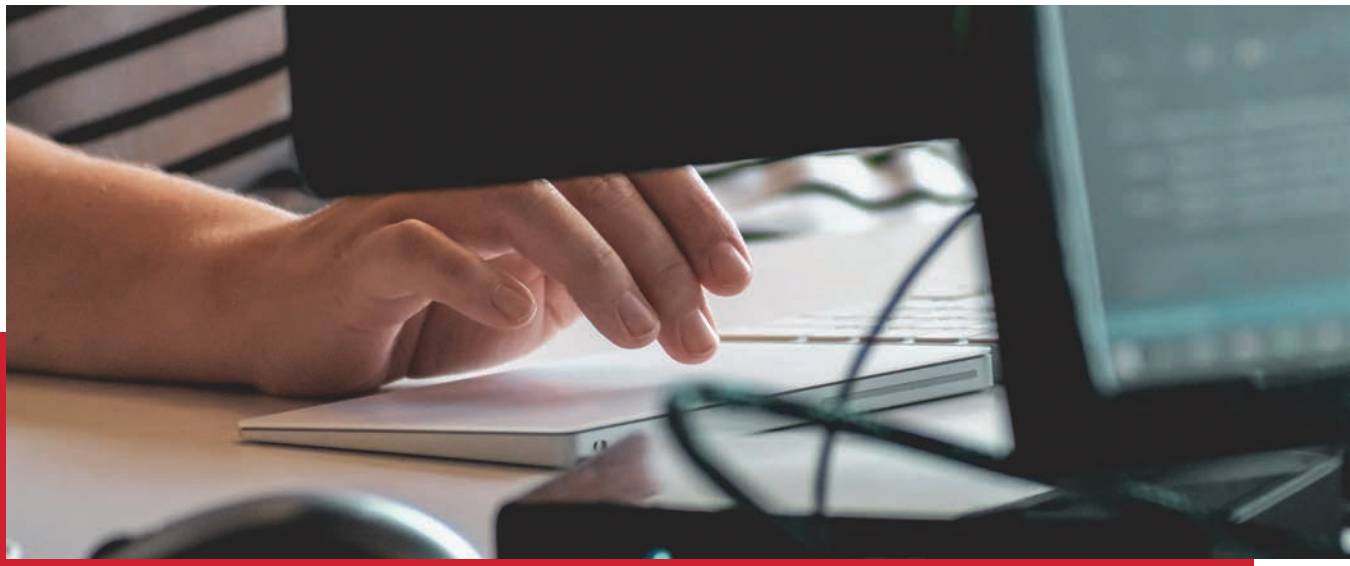
H. What will we do to prevent future breaches?

5 The breach is mitigated; but your work isn't done.

Information sharing is key to preventing others from falling victim to a similar attack. Publicize lessons learned and any important information uncovered during the event.

Penetration testing services can help you identify, prioritize, and remediate your security vulnerabilities and help validate whether your existing security controls are working as intended.

CONNECT WITH NETSPI TO GET STARTED!



ABOUT NETSPI >> NetSPI is the leader in enterprise security testing and vulnerability management. We are proud to partner with nine of the top 10 U.S. banks, the largest global cloud providers, and many of the Fortune® 500. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We uniquely deliver Penetration Testing as a Service (PTaaS) through our Resolve platform. Clients love PTaaS for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. We find vulnerabilities that others miss and deliver clear, actionable guidance allowing our customers to find, track, and fix their vulnerabilities faster.

To learn more, email
sales@netspi.com
or call us at
612-465-8880