3 Cyber Security Insights from V2's Cyber Roundtable

No longer a technology department problem, cyber risk responsibility rests in the C-Suite.

V2 Technology's Cyber Advisory Council held its inaugural event bringing together small and medium-sized business (SMB) leaders to learn more about Incident Response Planning (IRP) for managing a cyber incident. Depending on the scope of your business an IRP can be simple and implemented gradually over time. "Business owners should consider cyber a significant risk to their business and need to know what to do when it happens. We are bringing a holistic approach to cyber security to help owners mitigate these risks," advises Patrick Golembiewski, Council founder and CEO of V2 Technology.

1. It is not IF, but WHEN, so be PREPARED

As cyber incidents continue to climb, SMBs remain the single largest target for ransomware attacks. The average business disruption lasts 23 days. V2's Resident-CIO, David Howard states, "This (cyber disruption) is not something you want to think about on the fly, as it could be very dangerous for your business." Businesses need an executable plan that enables them to respond to an incident in the fastest, most thorough way possible. Policies, procedures, and tools should be required to be in place, allowing leaders to be prepared to handle issues and alert and inform internal, as well as external, stakeholders. Each role has its own responsibilities:

- **IT**
  - Deploy tools, alerts, procedures and policies including firewalls, antivirus, anti-malware, and patching to ensure preparedness.
  - Understand backup strategy/process — what is needed to support business continuity and password and access policies.
  - User security training is crucial. Teach users how they potentially enable breaches, what suspicious activity looks like, and how to go about reporting it. (Cyber security is often likened to securing a house. If the doors, windows and keys provide access, don't leave the doors and windows open or give the keys to the bad guys. Deny them access!).
- **Legal**
  - Identify laws and regulations businesses need for compliance.
  - Regulation requirements may be flowing down to other industries, so know the span of impact.
  - Identify all legal obligations and get your business in the best posture to be ready for an incident.
  - Review third-party contracts to know what you are signing, what you are agreeing to and make sure it is/they are included in the IRP and it is/they are accounted for.
- **Finance**
  - Know who to call – the knowledgeable internal and experienced external experts who can help.
  - Understand reporting requirements and financial safeguards that must be in place to mitigate risk.
  - Ensure proper entitlements are in place for designated accounts that provide the right checks and balances and ensure identity is verified.

- **Insurance**
  - Secure the proper level(s) of cyber insurance to support your business against attack and, in the event of an attack, during recovery.
  - The application process may reveal certain technical gaps that need to be filled to obtain the necessary coverage.

A prepared, written plan allows your team to understand exactly what recovery looks like when you are shut down after a cyber incident. According to Kyle Johnson, Partner, Brennan Manna Diamond, "An appropriate incident response plan may reveal gaps in your team, gaps in your contracts and gaps in your IT capability that you need to understand and fill in order to be ready."

2. Your TEAM makes a difference during a Cyber Incident

Teams are built to support multiple areas of the business. Cyber is NO exception. From detection of a cyber incident through recovery, everyone has a role. This includes your leadership, IT team, insurance broker, banker, and lawyer. Each role will execute the plan when you experience an incident. The right level of communication — and transparency — throughout is paramount!

User Community

Users play an important part in reporting suspicious activity. They may be the first to notice questionable activity. Create an informative and empowering culture for users to have a curious mindset and can confidently report suspicious activity. They may also provide data related to the incident that could be helpful in assessing the location of the breach.

IT Team

Often the first call made in the event of a breach, the IT team is perhaps the most critical group throughout all phases of a cyber incident. They start by assessing the impact of an incident — what happened and where is the impact? Does it affect one user or many? Is there financial loss? The team investigates what caused the incident and gathers necessary data. It is highly probable that members of senior management will need to participate in the assessments. Through the containment and eradication phases, support will be provided to isolate the incident, remove the compromised assets/user, eliminate the sources of the compromise, and prevent future breaches.

Legal Team

The next call is to your legal team. Legal helps to control the messages and manage the communication channels when stakeholders are alerted. Third-party vendors may need to be engaged and law enforcement involvement may be required depending on the scope of the incident. Attorney/client privilege allows for discussions about legal obligations and the prospect of planning for potential litigation as soon as

possible. Additionally, your legal team may have an incident or breach coach to support certain types of attacks. With regulated industries, handling system information and preserving logs enables better information for legal obligations related to the incident.

Finance Team

The finance team helps with the analysis and reconciliation/containment of funds associated with an incident.

Insurance Team

Your cyber-insurance policy should outline what is covered. Additional forensics may be needed and covered by your policy. Throughout the insurance (and legal, for that matter) process, it is important to know that words are very important when describing a cyber situation. For example, cyber attacks start as an "incident," not a "breach." Todd Lancaster of Oswald Companies warns that "The word breach can be a major flag for an insurance carrier…" and lead to additional scrutiny.

Recovery

"Recovery from a cyber incident or breach is dictated by how well you prepare for one," shares Brandon Pauley, Principal, Brennan Manna Diamond. Recovery steps include:

- Getting access to the cash, reconciling accounts to ensure all monies are accounted for.
- Understand the recovery and return times are for the business to set expectations with employees on how long it will take.
- Restoring systems, access, and backups.
- Go back to the detection phase to rescan what you brought back from the backups and make sure it is clean.
- Work to inform stakeholders (customers and vendors) about the situation and communicate to restore an organization's reputation.
- Build an insurance claim — there may be a lag until when you get the claim paid, this needs to be understood.
- Details and quantification will be necessary for an insurance claim, also claims advocates may be available to assist.
- Some businesses need to involve a third party (a forensic resource) to help investigate the incident to quantify the recovery.

Putting resources behind cyber threats and understanding the changing market of your business are critical. Information Technology spend is often seen as an expense item, not a revenue driver. A little investment in IT can go a long way to mitigate cyber risks.

3. TESTING the plan is critical

Preparation is key, but practice makes perfect when it comes to responding to a cyber incident. The bad actors are constantly evolving and seeking easier ways to win, so your plan needs to be rehearsed and adjusted on a regular basis – minimum annually. Whether you create the simulated attack and walk through the plan with your team or conduct an orchestrated table-top simulation, all the key stakeholders in responding to an incident need to know what to do when it happens. This includes testing backups and

measuring the response time to the attack. In some industries an annual penetration test may be required to assess readiness.
Your incident response plan should become a living document within the organization – just like other important policies and procedures. Lessons learned from each test will further improve your ability to respond.

In SUMMARY
Business owners need to build a cyber security incident response plan based on specific vulnerabilities within their business… the users within the organization, the systems and the data. It is NOT something to print off the internet and put in place. It requires involvement and input from many members of your internal and external team for a custom response.

** V2 Technology formed the **Cyber Advisory Council** to serve as a cyber security thought leader within the community – collaborating on current issues and providing support to SMB leaders in managing their risk within their business. Using a holistic approach, V2 has brought together key stakeholders from various industries in its fight against cybercrime. The Council includes representation from information technology, legal, banking, financial, insurance, and law enforcement industries. Specific members include: V2 Technology, Brennan Manna Diamond, Westfield Bank, and Oswald Companies, with input from the FBI.*