The Future of Cyber Crime Response

By Future Point of View

FPOV FUTURE POINT OF VIEW

Cyber crime presents the greatest transfer of wealth in human history, estimated to cost the world $10.5 trillion annually by 2025. Cyber crime has increased 600% during the pandemic, so developing proactive cybersecurity practices is key to mitigating risk and containing damages.

Increasing Cyber Danger

With the pandemic forcing companies to move to remote operations, cyber criminals have a greater attack surface with numerous weak points to exploit. Each employee working from home offers a new end point for a cyber criminal to attack, and there's always the risk of a device containing confidential information being stolen.

Employees and businesses are doing more online communication, with increased data and digital document sharing and increased use of video conferencing. Businesses are sending more data to more vendors, relying on these third parties' cybersecurity, and many are moving data to the cloud. All these online processes create more risk. There is also a steadily increasing threat of a ransomware attack: in 2021, 37% of all business and organization were hit with ransomware.

The Future of Cyber

Technological advancements deliver benefits as well as risks. Individuals can communicate with almost every other person in the world, but this also means that anyone can be harassed or attacked digitally. While everyone has a voice on the Internet, there is an associated danger of disinformation. Online surveillance and facial recognition provide proactive security, but also gives governments and security companies extreme power. Machine intelligence helps authorities pursue criminals, but the criminals put the same technology to their own nefarious uses. Drones are a great boon to photographers, hobbyists and online retailers using them for deliveries, but drones also support terrorism and spying. And when everything is a computer, from our kitchen appliances to our cars, we enjoy much more functionality, but live with much more risk because everything is now hackable.

Key Steps to an Effective Digital Incident Response Program

Given the burgeoning cyber risks and increased sophistication of cyber criminals, businesses should no longer consider *if* they'll face an incident, but *when*. Preparing in advance for the inevitable will position you to respond quickly and effectively to a digital attack or event.

In preparing for an attack, businesses should not assume they are completely safe, or rely solely on their internal technology team to evaluate security risk; instead, get a third-party opinion regularly, and don't use the same vendor year after year. Once you've invested the time to gain a complete understanding of your security risk areas, you can then obtain cyber insurance to help cover them.

Finally, build a comprehensive Digital Incident Response Program that incorporates executive training, tabletop scenario exercises and multiple playbooks, one for each type of potential attack; FPOV has developed 40 different playbooks. It's important to keep in mind that the incident response program is not a checked box, it's a moving target that will require regular updates to incorporate new risks and improved responses.

Digital Incident Response Playbook Checklist

Each playbook should include plans and instructions for three phases of any digital event, from a stolen device to a ransomware attack. Tabletop scenarios should follow, and executive training address, these same phases.

Phase 1: Discovery, Plan and Severity: The first step in any response is to verify the breach or incident, and what data is at risk or has been stolen. Once the event is defined, the appropriate playbook is brought into action. All roles and responsibilities are identified, as are outside vendors such as a cybersecurity firm or bitcoin broker in case of a ransomware attack. These vendors don't need to be on retainer, but you should establish a relationship so they're ready to offer support when an event occurs.

Phase 2: Communication, Containment and Forensics. The response team needs a secure line of communication outside the scope of the event – for example, if the company's email system is attacked, you wouldn't want to use email to communicate. Specific, approved language regarding the breach should also be employed, with defined messaging for different audiences including regulators, investigators, customers and employees. The priority and scope of communication is also important, addressing questions like is the first call to the lawyers, does the board need to be involved or when should you contact the cyber insurance provider.

Phase 3: Remediate, Recover and Best Practices: Once the attack has been resolved, it's time to undertake reputation management activities and develop long-term messaging for your various audiences. You should also conduct a final financial analysis and file the relevant insurance claim. And finally, use all the documentation from the first two phases to conduct a post-mortem exercise, identify playbook improvements and define new best practices to employ.

Financial Risk Management

Cyber insurance is now available to cover some damages from some digital attacks. Often, this insurance policy is the most important means to make up financial losses. Given the fluidity of technology developments, cyber insurance can change from one policy year to another, so be sure to read each new policy carefully and identify what's changed.

Cyber policies often have detailed clauses and exclusions making successfully filing a claim a challenge. For example, a policy may require you to use certain forensic professionals, lawyers, crisis management people and/or their choice of bitcoin broker; if you don't, the carrier may deny the claim. They may also deny a claim if an outage was too short, as defined by the policy, or pay less for a social engineering

attack versus a hacking event. For this reason, you should have an insurance expert help review your policy and file any claim, whether that expert is an employee or a trusted vendor.

While cyber insurance is ever-changing to match the technology and risk landscape, it is also becoming more expensive. There will be fewer providers and less coverage in the marketplace because people won't be able to provide the detailed underwriting the insurers need. States are enacting more and more regulations, which lead to more exclusions, so policies may become less of a mitigation even as premiums increase. Already, some carriers won't underwrite a company that does not have a digital incident response program, making this critical preparation step even more critical.