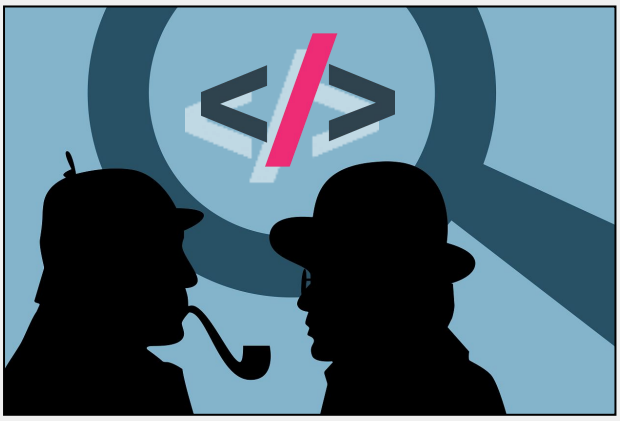
Hippogriff LLC - Forensics Review Fast Look

When device tampering, data exfiltration, information manipulation, financial transaction theft, blackmail, eavesdropping, espionage, or threatening instances happen to individuals or organizations, a complete forensics inspection of Software, Hardware, and Human Domain variables must be carried out; remotely and on premises if need. There are many steps that must be taken, and all of them are vital to the outcome of such investigations.



Why are these steps necessary, non-negotionable, and often times required by law?

- Reporting a cyber incident (if necessary) to authorities, insurance, vendors, partners, and customers is not only a ethical and operations survival necessity, it is also required under state and federal compliance mandates.
- Insurance will be more likely to increase the available coverage to a policy holder over time – when the policy holder proves to insurance that they have a law enforcement case number on file; hence re-enforcing the urgency of a crisis response claims situation.
- The legal representation of an affected organization will have more supporting material to stave off class action lawsuits or regulatory fines by presenting an insurance claim number to inquiring entities. This shows due diligence responsibility – as the involvement of an entity which is "supposed to perform" a risk analysis of a policy holder before granting coverage has their reputation and focus of liability drawn into the cyber incident intervention.
- Consumers, non-profit donors, investors, or share holders are not the only ones affected by cyber incidents; the internal employee base and any sub-contracted or volunteer staff are also often times exposed to harm in these circumstances, and this increases the legal, financial, and sociological ramifications that business owners and managers will face in a court of law and in the court of public opinion.

All of these elements, and the steps to climb the mountain of incident recovery, prove responsible action on the part of the policy holder/victim/affected organization – thus decreasing the plethora of consequences due to Information Security (InfoSec) incident fallout.

What needs to happen after a malicious or negligent cyber incident? The usual process of response includes:

1. Victim contacts law enforcement to receive a Case Number...
2. Victim contacts insurance provider to receive a Claim Number...
3. Victim contacts InfoSec firm – Hippogriff – for assistance...
4. Victim undergoes consultation with Hippogriff...
5. Victim reviews initial quote from Hippogriff...
6. Victim signs Hippogriff Sales Purchase Agreement for confidentiality, liability, etc. – needs...
7. Victim assists Hippogriff in formulating a Timeline of Events for insurance submittance...
8. Victim receives revised quote from Hippogriff as more details emerge/divulged on the situation...
9. Victim's insurance provider reviews Timeline of Events to assess if policy compensation may be released...
10. Victim signs Hippogriff's Statement and Scope of Work Agreement...
11. Victim's insurance provider releases initial tranche of compensation for Forensics IT Review and Systems Remediation...
12. Victim pays Hippogriff for initial portion of Statement and Scope of Work Agreement...
13. Victim's systems are investigated and corrected by Hippogriff technologists...
14. Victim awaits Hippogriff Incident Response Report and packaging of forensics findings to be mailed to insurance (if applicable), this includes any vendor subpoenas written by Hippogriff on behalf of client...
15. Victim's insurance reviews Hippogriff's findings and then concludes if legal assistance is now required to report the cyber incident to consumers, state attorney general's office(s), etc. – or otherwise...
16. Victim's insurance expands upon dialogue to consider the release of additional compensation funds for the remediation and continuation process to stave off any further cyber incident...

Every cyber incident is different, and how an organization responds will determine how severe, or not severe, the harm will be. Rapid communication is required by victims – so that every possible avenue can be entertained to regain the trust and operational capability that consumers and citizens alike are expecting. Follow instructions and come out on top; ignore reality and its seriousness – and suffer a dire conclusion.

Computer Technology Protection Services

1-866.273.4831
inquiry@hippogriff.tech
Hippogriff.TECH • Hippogriff.IO