Services We Offer

Data Breach Investigations

- Retail, credit card theft
- Intellectual property theft
- Internal corporate investigations

Incident Response

- Attacks on corporate networks

Digital Forensics

- Private investigations support
- Data recovery

Training

- Prepare and plan for data breaches and cyber attacks
- Initial response and triage

Consulting Services

- Cyber security and APT consulting
- 1099 staff augmentation

Why us?

Twenty years of IT experience; over fifteen years exclusively performing forensics and response

Provided cyber services and support to small businesses and Fortune 500 companies alike

Provided extensive forensics and investigation support to the Department of Defense and the intelligence community

Questions?

Email: info@brimorlabs.com

Phone: 443.834.8280

BRIMOR LABS

Data Breaches, Incident Response, Digital Forensics, and YOU

Visit us on the web: ***www.brimorlabs.com***

Why Data Breaches Happen

Cyber attacks are unfortunately common and all businesses will experience them.

We've regularly seen attackers exploit these areas:

1) Outdated, unpatched, and/or unsupported software and devices present on the network
2) Lenient password policies (not requiring strong/complex passwords or implementing enterprise-wide resets when needed)
3) Lax "Bring Your Own Device" (BYOD) policies that spread malware to the network
4) Development or temporary servers that are left unpatched and forgotten
5) Not limiting access (internal and external) to the network and allowing everyone to see everything
6) Ineffective physical security practices (access to the server room bypasses most technological barriers)
7) Utilizing 3rd party vendors/suppliers who do not follow good security practices

Small Businesses Shoulder the Heaviest Burden

Nearly 2/3 of data breaches affect small businesses

Direct costs are expensive:

- Regulatory fines, lost revenue, lawyer fees, credit monitoring, insurance premiums, mandated notification costs, new or repaired network infrastructure, incident response and data recovery services

Indirect costs are also expensive:

- Brand and reputation damage, lost time and productivity, public perception

The average overall financial impact of a cyber attack is nearly $3 million.

- Typically $188 per record compromised
- Typically $355 per health care record compromised

Customer Data

Corporate Data

Financial Information

Intellectual Property

What Should Small Businesses Do?

1. If you fail to plan, you plan to fail. Have and practice an incident response plan and know when to call a professional.
2. Regularly train employees on information security best practices.
3. Regularly conduct vulnerability assessments.
4. Change default settings and passwords on all devices and software.
5. Enable automated alerts on ALL unusual activity.
6. Enable thorough logging and review the data. If you use a 3rd party IT company, insist on having access to YOUR logs.
7. Update all software and devices as recommended. Restrict or prohibit use of personal devices on your network.
8. Segregate your network. (Don't store financial data on the same network where employees use social media.)
9. Regularly backup relevant information; but if you no longer need it, destroy it.