AMON TECHNOLOGIES LLC

CYBERSECURITY STRATEGY

AREAS THAT NEED BOARD ATTENTION – 1

- Take steps to prevent damage caused by IT being compromised
- Protect corporate and financial data and trade secrets,
- Protect shareholders, customers, suppliers and staff information
- Properly plan for responding to cyber threats

AREAS THAT NEED BOARD ATTENTION – 2

- Cyber security resilience needs same attention as financial & operation health.
- Board (not IT) needs to set parameters of cybersecurity policy at a strategic level.
- Oversee the formulation, activation, implementation, monitoring and maintenance of cybersecurity policy.
- Never underestimate complexity and cross cutting impact of cyber threats

RECOMMENDED BOARD CYBERSECURITY ACTIONS

- Adopt A Structured Methodical Approach
- Undertake Detailed Cybersecurity Assessment
- Prepare A High Level Cybersecurity Strategy
- Identify And Prioritize Cybersecurity Projects
- Secure Necessary Budgets
- Implement In Accordance With Priorities

BUSINESS ASSET PROTECTION

- Customer information
- Product information
- Intellectual property
- Financial data
- Banking information
- HR information
- Corporate information databases

BUSINESS OPERATIONS DAMAGE

- Loss of competitiveness
- Compliance breaches
- Damaged reputation
- Loss of productivity
- Financial loss
- Intellectual property loss

TRADITIONAL IT SECURITY STEPS

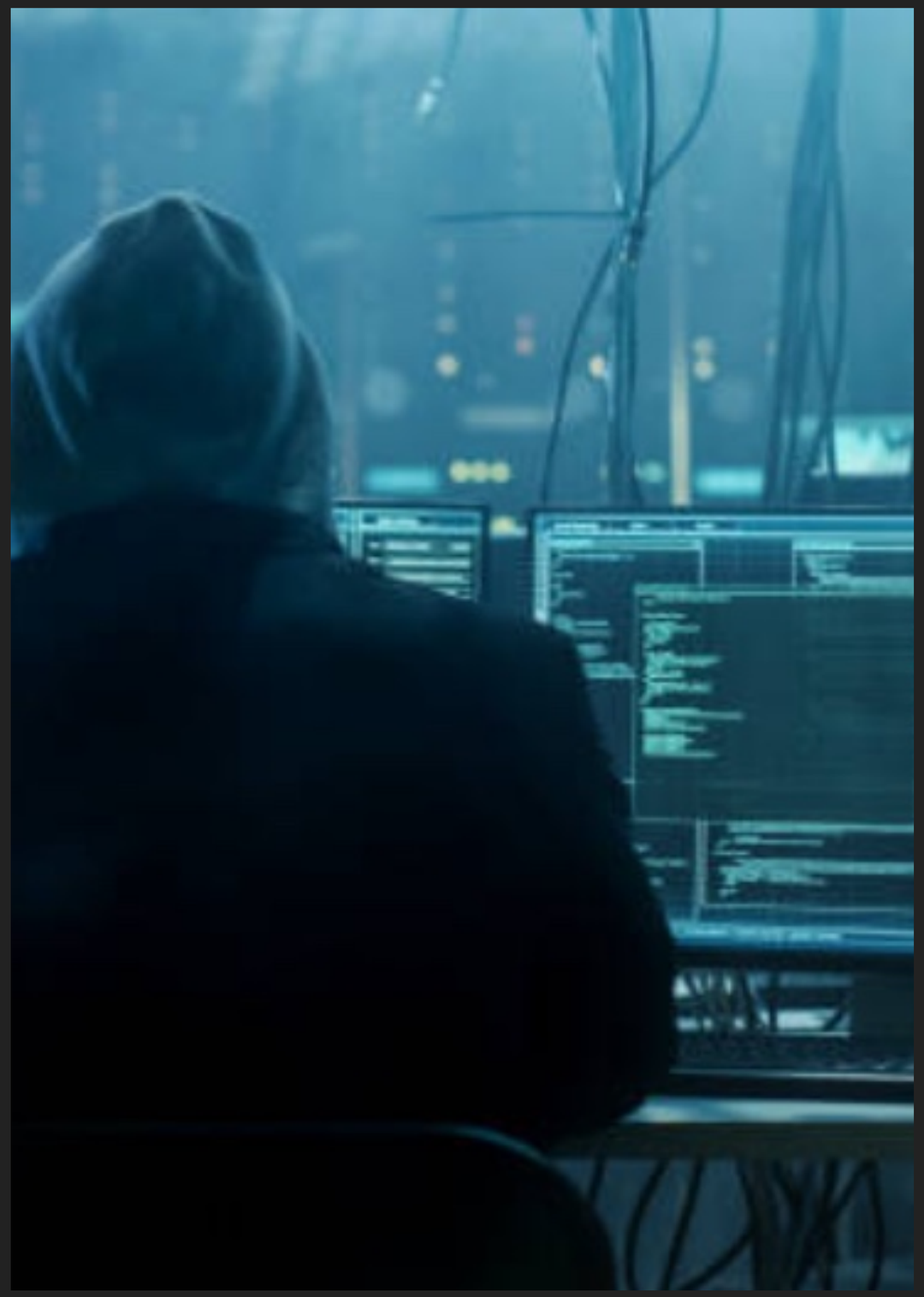
- Avoid using unsupported software
- Install latest software updates
- Run up to date anti-virus software
- Use strong passwords
- Delete suspicious emails
- Back up data
- Train staff on IT security awareness
- Manage security relationship with suppliers

UPGRADE CYBER SECURITY

- Close gap between traditional protection and sophisticated cyber attacks
- Use signature-less threat protection
- Complement existing Firewalls and IPS
- Identify, contain and block cyber attacks
- Real-time analysis of web traffic

DELEGATE FIREFIGHTING OUT OF IT

- Avoid reactive actions to attacks.
- Proactively block malware from reaching users and servers.
- Reliance on anti-virus Solutions is not enough.
- Signature based systems are impotent in stopping zero day and other targeted attacks.
- Significantly reduce downtime.



DELIVERABLES

- Cyber security assessments
- Cyber security strategies
- Technical & functional specs
- Cyber security tenders & RFPs
- Systems and services selection
- Project management
- Implementation Supervision

Q & A SESSION

Vatche Dakessian / CEO