LET AES BE YOUR CHIEF INFORMATION SECURITY OFFICER

SECURITY BASICS

Cyber-Security in practice can be exceptionally complex, but its essence is quite simple. It is nothing more than reducing or taking away risks. Experience shows that the most hacks (about 90%) are still using the simplest methods and weaknesses. Companies need to create and fortify basic cyber security solutions for these simple risks. Our process involves avoiding security system problems in the first place. We improve the odds of never having a catastrophic breach by making sure your basic cyber-security and policies are being fully implemented and enforced.

The best incidents are the ones that never happen.

One of the main cyber-risks is to think they don't exist.

The only system which is truly secure is one which is switched off and disconnected.

THESE INCLUDE:

- Firewalls
- Intrusion detection systems
- Security Incident and Event Management (SIEM) systems
- Automated security monitoring and alert orchestration systems
- Spam Filters & Anti-Phishing
- Access Control – Identity and Access Management (IAM) and Privileged Access Management (PAM) for back-end administrative access
- Strong passwords & two-factor authentication
- Encryption of sensitive data as required by regulation and policies (at rest and in transit)
- Security software for smartphones
- Antivirus systems, updated real-time and set up for continuous protection
- Regular backups, stored offsite.

AES ADVANCED ELECTRONIC SOLUTIONS, INC

Driving Security Innovation

RISK ASSESSMENT

Our risk assessment doesn't only fine-tune your cyber-security response, but also helps prevent attacks in the first place. It involves putting yourself in the mind of an attacker. We identify what may be most valuable to them thus allowing us to focus resources to protect the most vulnerable assets/data.

PLANNING

We help in developing your Incident Response Plan. We'll refer to the most recent changes in your plan and most current threats and regulations. We recommend the latest improvements, training, and preparation so your teams know how to act as soon as a threat is detected. Cybersecurity threats are evolving all the time. That's why it's important to be proactive. Improvements, training, and preparation need to be completed before the next major breach attempt. Each plan should be tested and kept up-to-date. Outdated incident response plans are likely to be ineffective.

EXECUTION

Network Security

Enable operating system firewalls where available

Install a stateful hardware-based firewall

Configure firewall rule sets to be very restrictive

Application Security

Examine changes required to support encrypted databases

Modify software to work with encrypted data

Safely store and protect the encryption keys

System Security

Remove user privileges to install software

Remove unsafe software from workstations

Establish a process for the evaluation of new software

Operational Security

Evaluate and Train on existing security best practices

Audit systems & procedures ensuring compliance

AES ADVANTAGE

AES is one of the New York largest privately held Security Systems Integrators. AES' track record of developing solutions for a wide range of customers has given us the opportunity to gain deep insight into key industries and business sectors. Consequently we provide a comprehensive array of solutions which include: Access Control, Fire & Life safety, Datacomm, Intercom, DAS, ARCS, Covert & TSCM, IP Video, Cyber Security and Health Monitoring

AES ADVANCED ELECTRONIC SOLUTIONS, INC

Driving Security Innovation