AITHERAS

CUSTOMER-CENTRIC INNOVATIVE SOLUTIONS: CYBERSECURITY

CYBERSECURITY CHALLENGES

HOW AITHERAS SOLVES THEM

STRATEGY WEAKNESSES

Strategies fail to efficiently address collective risks and weaknesses in all areas including emerging technologies, workforce management, and malware.

→

1

We develop and execute a comprehensive strategy that mitigates global supply chain risks, addresses cybersecurity workforce management challenges, and ensures the security of emerging technologies.

REACTIONARY PROCESSES

Since events, alerts and issues are solved in a reactionary manner today, it is often difficult for agencies to get ahead of emerging threats.

→

2

We utilize an SSAE-18 compliant data center from which we operate a Security Operation Center (SOC). This gives you 24/7/365 Real-time security monitoring, alerting, and response. We conduct risk assessments, threat protection, and vulnerability scans and assessments.

SLOW ACQUISITIONS

Because of the necessary due diligence, vetting and bidding it means that even critical security upgrades could take 12–18 months.

→

3

Our highly skilled security experts possess impressive backgrounds in government contracting, program and project management, information and personnel security, risk and vulnerability assessments, and national and international security operations management, to save you time.

CONTRACT VEHICLES

- Department of Justice Data Analytics Solution BPA GS-35F-494GA
- GSA Schedule Contract IT 70-GS-35F-0068S
- GSA Schedule 36 – GS-03F-034DA
- National Institute of Health CIOSP-3 Large and Small
- U.S. Army Corps of Engineers (USACE) Automated Controls and Cyber Security Systems (ACCS) Engineering and Design Support for USACE Hydroelectric Design Center
- 8(a) STARS II – Contract Number GS00Q17GWD2073

DESIGNATIONS

SAM Active
Certified Minority Business Enterprise
ISO 9001:2015

51 Monroe Place, Suite 506, Rockville, MD 20850 . 800-592-5436 . contact@aitheras.com . aitheras.com

AITHERAS

CUSTOMER-CENTRIC INNOVATIVE SOLUTIONS: CYBERSECURITY

OUR SERVICES AND PRODUCTS

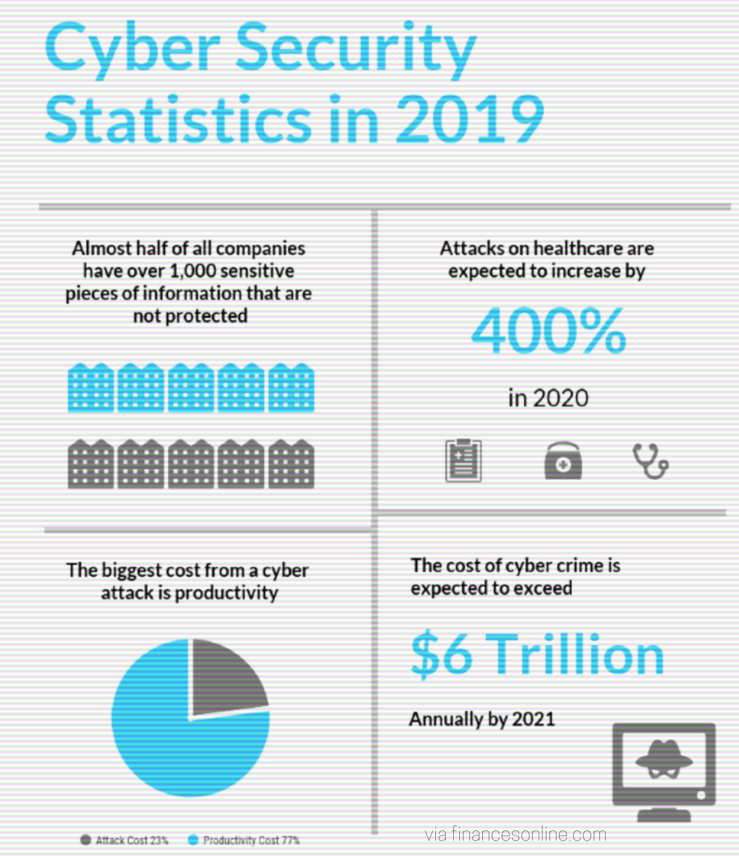
Managed Security Services
- Continuous Security Monitoring
- Log Management
- Intrusion Prevention & Detection
- Managed FirewallVulnerability Remediation

Risk Assessment
- Penetration Testing
- Vulnerability Assessments
- Audit and Compliance

Industry-Specific Security Services
- HIPAA Compliance and Testing
- SSAE 18 Audit Preparation
- SCADA Implementation
- HIPAA and PCI Compliance Services

Threat Protection
- Threat Intel
- Security Awareness Training
- DDoS Testing and Mitigation
- Data Loss Prevention

Incident Management
- Incident Response
- Forensic Analysis
- Malware Reverse Engineering



Cyber Security Statistics in 2019

Almost half of all companies have over 1,000 sensitive pieces of information that are not protected

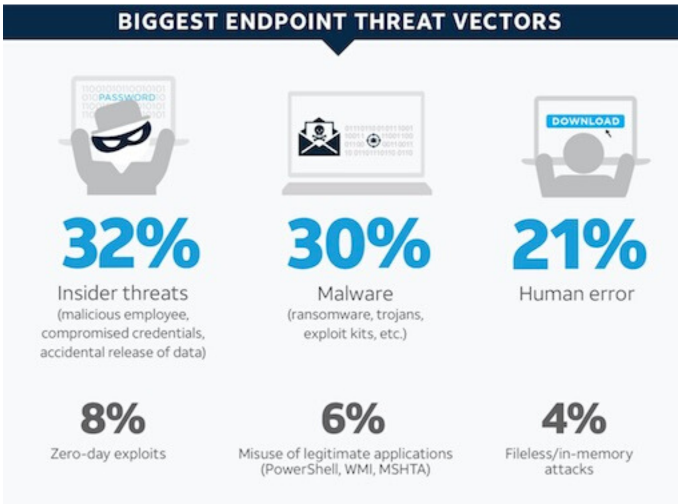
Attacks on healthcare are expected to increase by 400% in 2020

The biggest cost from a cyber attack is productivity

● Attack Cost 23% ● Productivity Cost 77%

The cost of cyber crime is expected to exceed $6 Trillion Annually by 2021

via financesonline.com



BIGGEST ENDPOINT THREAT VECTORS

32% Insider threats (malicious employee, compromised credentials, accidental release of data)

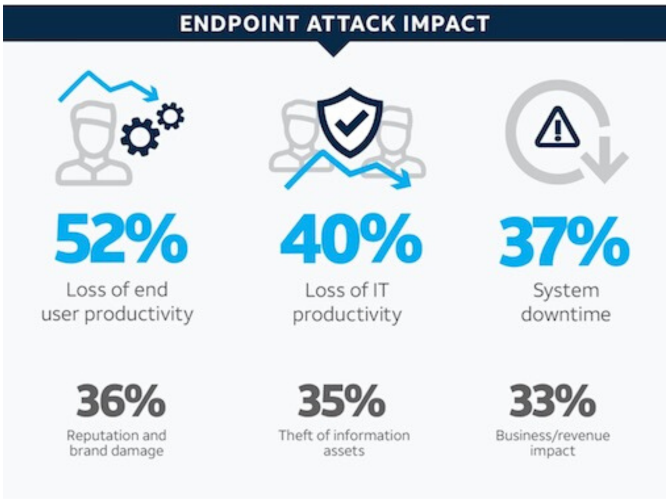
30% Malware (ransomware, trojans, exploit kits, etc.)

21% Human error

8% Zero-day exploits

6% Misuse of legitimate applications (PowerShell, WMI, MSHTA)

4% Fileless/in-memory attacks



ENDPOINT ATTACK IMPACT

52% Loss of end user productivity

40% Loss of IT productivity

37% System downtime

36% Reputation and brand damage

35% Theft of information assets

33% Business/revenue impact

via cybersecurity.att.com