Winning The Ransomware Game

Lisa Carter
SpartanTec, Inc.
www.SpartanTec.com

Who Is SpartanTec?

- Founded in November 2002
- Profitable from Day 1
- We are a Complete Technology Solution Provider – Evolving with the Environment
- We Focus on I.T. Security!
- Personal Service. We know our customers on a first name basis.
- Unbiased Security / Network Advisor

Concerns?

- ….about losing company data to a cyber attack?
- ….about the threats to your company data? Don't Become the Next Headline Statistic in the news.
- …what concrete steps can you take immediately to increase security?

SpartanTec
Incorporated

Today we're going to cover....

Why Cyber Crime is Exploding

How a Cyber Attack Affects your organization

Things You Can Do **TODAY**

Critical Layers of Security

SpartanTec
Incorporated

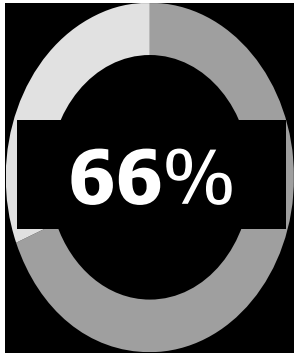
Cyberthreat Landscape

"Unauthorized software and devices, and stressed and distracted workers, have expanded the attack surface and left businesses exposed to a number of cyber-risks. Small and medium-sized businesses are most vulnerable since most of them run legacy or outdated systems. In such challenging times, management teams need to have strong oversight on the cyberthreat landscape."

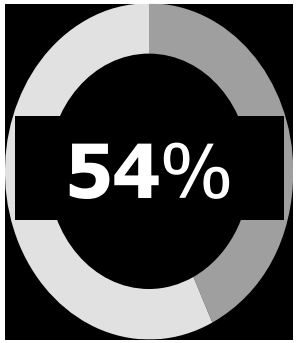
- Forbes

SpartanTec Incorporated

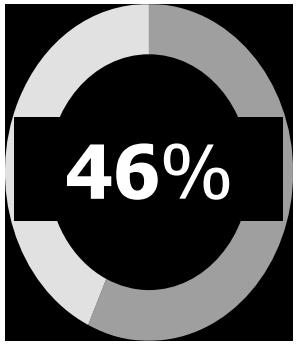
Continuing to mitigate risk is the top priority.



have not identified and documented cybersecurity threats



have a company-wide disaster recovery plan in place



have not informed and trained all users

SpartanTec Incorporated

* Based on anonymous data of over 1,000 risk assessments, 2021

Top CyberCrimes On The Rise...

Phishing Scams

Website Spoofing

Ransomware

Malware

IOT Hacking

SpartanTec
Incorporated

Victim Loss

- This number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by a victim.

- In some cases, victims do not report any loss amount to the FBI.

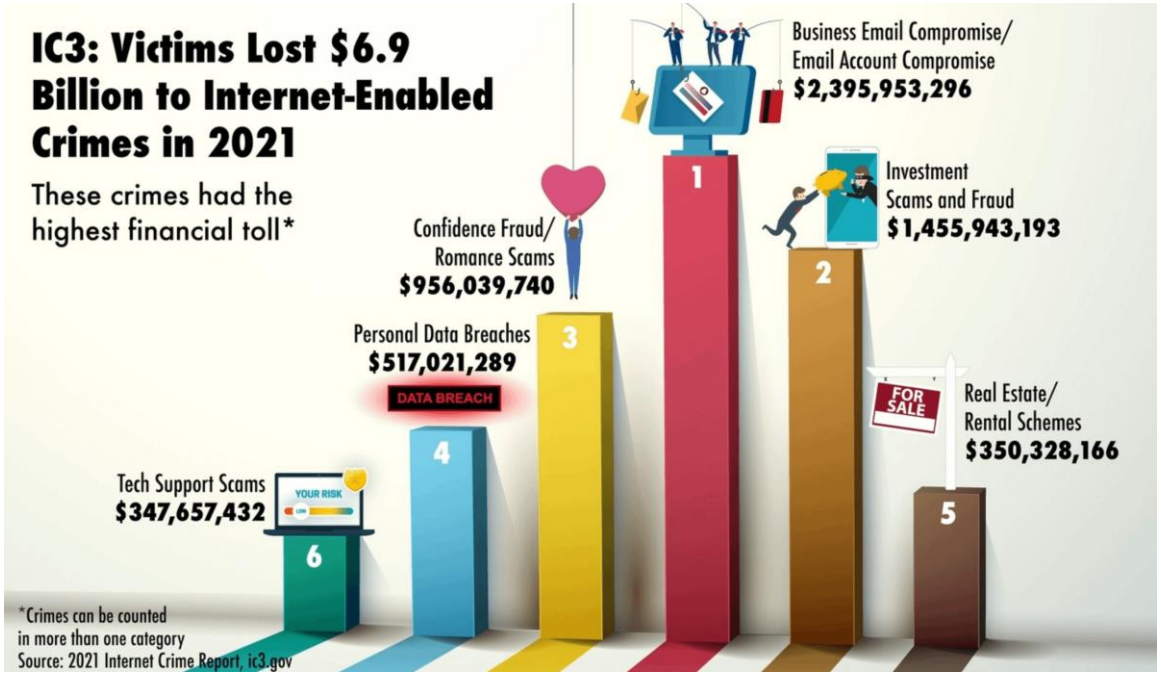
By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,866,642,107	Overpayment	$51,039,922
Confidence Fraud/Romance	$600,249,821	Ransomware	**$29,157,405
Investment	$336,469,000	Health Care Related	$29,042,515
Non-Payment/Non-Delivery	$265,011,249	Civil Matter	$24,915,958
Identity Theft	$219,484,699	Misrepresentation	$19,707,242
Spoofing	$216,513,728	Malware/Scareware/Virus	$6,904,054
Real Estate/Rental	$213,196,082	Harassment/Threats Violence	$6,547,449
Personal Data Breach	$194,473,055	IPR/Copyright/Counterfeit	$5,910,617
Tech Support	$146,477,709	Charity	$4,428,766
Credit Card Fraud	$129,820,792	Gambling	$3,961,508
Corporate Data Breach	$128,916,648	Re-shipping	$3,095,265
Government Impersonation	$109,938,030	Crimes Against Children	$660,044
Other	$101,523,082	Denial of Service/TDos	$512,127
Advanced Fee	$83,215,405	Hacktivist	$50
Extortion	$70,935,939	Terrorism	$0
Employment	$62,314,015		
Lottery/Sweepstakes/Inheritance	$61,111,319		
Phishing/Vishing/Smishing/Pharming	$54,241,075		

SpartanTec Incorporated

Business Email Compromise

Two common financial losses related to BEC:



1. Fraudulent transfers of money
2. Obtaining personally identifiable information of staff to use in future attacks

SpartanTec Incorporated

What is Ransomware?

ran·som·ware

/ˈransəmˌwer/

noun

a type of malicious software designed to block access to a computer system until a sum of money is paid.

A New Ransomware Attack Occurs Every **11 Seconds**

Approximately 1 Million Cyberattacks are attempted per day…..

SpartanTec
Incorporated

Government

In 2021, ransomware attacks on the government increased to three times the previous year's high point. (SonicWall)

In June 2021, there were about 10 times more ransomware attack attempts than average on the government. (SonicWall)

246 separate ransomware attacks struck U.S. government agencies in the last three years, costing close to $52.88 billion. (CompariTech)

SpartanTec
Incorporated

Ransomware Predictions and Future Trends for 2022

30% of organizations will adopt Zero Trust Network Access (ZTNA) models by 2024. (Gartner)

40% of boards of directors will have a cybersecurity committee by 2025 as stricter cybersecurity measures become a top priority. (Gartner)

70% of CEOs will invest in an organizational culture of cyber resilience by 2025. (Gartner)

IoT devices are predicted to be increasingly used by attackers to carry out ransomware attacks in 2022 and beyond. (RSA Security via Security Boulevard)

SpartanTec Incorporated

Cyber War Stories

1. No Security in place at all

2. Put Trust in the wrong people
- open WIFI
- active A/D accounts for long gone employees with big permissions
- no collaborative documentation – one person has all the information

3. No backups or backups aren't tested

SpartanTec
Incorporated

How Are You Keeping Your Company Out of the Headlines?

SpartanTec
Incorporated

Security Framework

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
What data is important to you? What level of tolerance do you have to lose any (all) of that data? How much downtime is acceptable?	Doors and Windows	Alarm	Dog	Do you have a tested business continuity plan (disaster recovery) plan? What department (or data) must be restored first? Do you have a communications plan?
	Locks	Motion Sensor	Baseball Bat	
	Fence	Doorbell Camera	Police	
	Yard Signs	Neighborhood Watch	Insurance	

SpartanTec Incorporated

Components of a Well-Designed Security Solution for your Organization

Security Assessment

Security Awareness

Passwords

DNS Protection

Mobile Device Security

Advanced Endpoint Detection & Response

SIEM / Log Management

Dark Web Research

Backup

Computer Updates

Spam Email

Multi-Factor Authentication

Encryption

Firewall

Cyber Insurance

Step 1: Identify

1. What data do you want to protect?

Data Owner?
Power Users?
Accounting & HR?
Business Line App?

2. What are the threats that could impact that data?

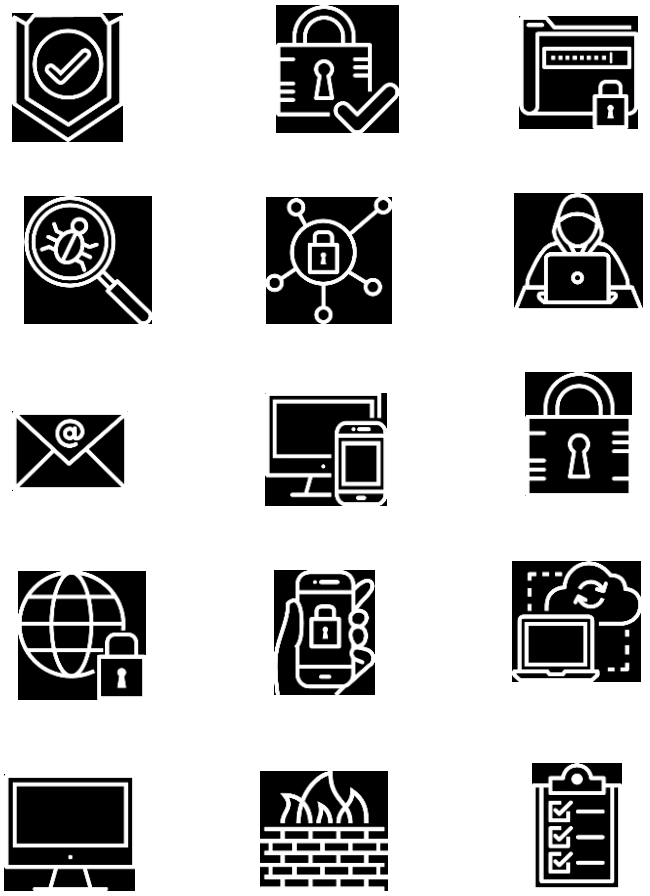
Cyber attack
Accidental deletion
Intentional insider
Spear Phishing

3. What is your current ability to detect and respond to those threats?

Downtime (per group)?
Lost revenue?
Missed opportunity?

Step 2: Protect, Detect & Respond

1. What boxes can we check?
2. Where are the gaps?
3. Which are the most crucial holes to fill today?
4. Are you comfortable with the remaining gaps?



Step 3: Recover (Survival)

1. Is your plan in place?
2. Have you tested the plan?
3. Does your team know their role and responsibilities?

FOX 5 WATCH NEWS SPORTS WEATHER SEEN ON FOX 5 CONTESTS BE OUR GUEST JOBS

Scripps CEO says cyberattack was result of ransomware; patient records to be restored this week

by: Dillon Davis
Posted: May 24, 2021 / 06:35 PM PDT / Updated: May 24, 2021 / 10:26 PM PDT

SAN DIEGO – The more than four-week disruption of services at Scripps Health was the result of a ransomware attack, the health system's chief executive said in a letter Monday.

Scripps President and CEO Chris Van Gorder apologized to patients, employees and physicians for the frustration caused by the attack which initially was detected May 1. The San Diego-based nonprofit system took a large portion of its network offline as a protective measure, resulting in rescheduled appointments for patients and some uncertainty for its staff.

Scripps employee says access to some internal systems now available amid cyberattack →

Chris Van Gorder, Scripps Health CEO, inoculated Christian Dollahen, 66 from Oceanside with the Pfizer vaccine at the Del Mar Fairgrounds on Friday, Feb. 12, 2021, in Del Mar, Calif. (Helvin C. Cepeda/The San Diego Union-Tribune via AP, Pool)

Let's Assess!

Firewall / Routers
Backup Systems
Cloud Services
In-House Servers
End User Systems
Networking Equipment
Cabling Structures
Backup Power Units
Printers / Scanner Vulnerabilities
Remote / Branch Office Access
Social Factors

Lisa Carter
lcarter@spartantec.com
843-418-4792

SpartanTec
Incorporated

Want to think about it?

Take a moment to test yourself with our Technology Success Scorecard.
www.SpartanTec.com/scorecard

SCAN ME

SpartanTec
Incorporated

Thank You for Attending Today!

SCAN ME

Phone: 843-418-4792

Lisa Carter
lcarter@spartantec.com

SpartanTec
Incorporated