SECUR-SERV + proofpoint.

CYBERSECURITY HAS CHANGED. HAS YOURS?

5 Cybersecurity Assumptions That Could Cost You

September 15, 2026

Presenter

Bill Szumski

Secur-Serv

VP, Support & Security Services

- 25+ years in IT and cybersecurity, specializing in security-first managed services
- Proven track record building and leading high-performing support and security teams in fast-paced MSP environments
- Leads the Secur-Serv team protecting 20,000+ endpoints for over 700 customers nationwide
- Let's Get Connected

  linkedin.com/in/bill-szumski

SECUR-SERV + proofpoint.

Presenter

Eric Townsend

Proofpoint

Global MSP Cybersecurity RMM Lead

- 2026: Spent over 900+ hours with SMB channel partners
- Involved with Cybersecurity For About 15 Years
- Worked with Various End Customers
  - Finance
  - Manufacturing
  - Retail
- Fun Fact: Avid Reader
- Let's Get Connected

  linkedin.com/in/ericdtownsend

FORZADASH MSP INFLUENCER 2025

Agenda

SECUR-SERV + proofpoint.

- Who is Proofpoint
- Secur-Serv Overview of Solutions
- Discussion About 5 Cyber Security Assumptions That Could Cost you
- From Theory to Reality
- Open Q&A

SECUR-SERV
+
proofpoint.

Secur-Serv + ProofPoint Partnership

proofpoint. Partnership

SECUR-SERV + proofpoint

Partnership Value

Part of Security Partner Suite

Bundled Management & Full Support

Key Component of Full Security Stack

Helping stop threats with enterprise grade security infrastructure for over a decade

Security Operations

SECUR-SERV + proofpoint

Managed Security Services

SECUR-SERV + proofpoint

Managed Security Services

60%
cost reduction by outsourcing over in-house cybersecurity staffing

- Cybersecurity Awareness Training
- Password Management
- Security Operations Center (SOC)
- Multi-Factor Authentication (MFA)
- Mobile Device Management
- **Email Security & Compliance**
- Managed Detection & Response (MDR)
- Endpoint Security (EDR)

SECUR-SERV
+
proofpoint.

Who is Proofpoint?

1 in Every 3 Business Emails
Proofpoint Sees

SECUR-SERV + proofpoint

3.4 trillion emails scanned per year = 9,315,068,493 emails scanned a day

Market Adoption

>2M+	1.74M	10k	85%	>60%
Customers	Small & Medium Businesses	MSPs Using Proofpoint		

FORTUNE 100

85 of the Fortune 100 & ConnectWise Uses Proofpoint

Proofpoint's Data

People Protection

3.4T	>1.4T	0.8T	21T
Emails scanned per year	SMS/MMS scanned per year	Attachments scanned per year	URLs scanned per year

2.2B	138M	395M
Phishing attacks stopped last year	BEC attacks stopped last year	Telephone Oriented Attacks stopped last year

85 of the Fortune 100
Use Proofpoint

SECUR-SERV + proofpoint

World Class Customers with Office 365 Trust Proofpoint

Poll Question #1

How are most cybersecurity attacks started?

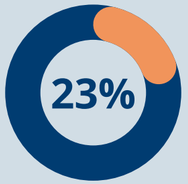
- Email
- Compromised websites
- Unpatched software
- Stolen devices

Poll Question #1

How are most cybersecurity attacks started?

- **Email**

91% of targeted attacks start with email



of people will always click.
This makes humans the weakest link in the security chain.

SECUR-SERV
+
proofpoint.

What Changed While You Were Running the Business

Cybersecurity Assumptions

SECUR-SERV + proofpoint

Subject: Confidential and Urgent!!! Urgency

Hi Chris,

I need your help with something that's both confidential and extremely urgent. Urgency

Please respond by email ASAP, Urgency I cannot take calls.

Regards,

Frank

Frank Wright
CEO

Would your current security tools stop this?

- ⚠ No malware
- ⚠ No attachments
- ⚠ No obviously malicious URL

Cybersecurity Assumptions

SECUR-SERV + proofpoint

Technology changed.

Employees changed.

Work changed.

AI changed.

Attackers changed.

But many cybersecurity strategies haven't.

What are you doing to make sure yours is keeping up?

Poll Question #2

How much have AI-generated phishing emails increased?

- 325%
- 750%
- 1,000%
- 1,265%

Poll Question #2

How much have AI-generated phishing emails increased?

1,265%

Remember, 91% of attacks start with email

The Risk Is Already In Your Environment

SECUR-SERV + proofpoint

68% of employees use AI tools IT never approved

50% of organizations expect AI-related data loss within 12 months

47x AI tools found vs. approved in a real enterprise

Employees have deployed AI tools in all varieties of form factors your security team doesn't know about.

Shadow AI, browser copilots, personal ChatGPT, all touching corporate files and data outside any policy.

Agents are creating automated workflows and MCP connections outside your architecture review.

Every SaaS integration, every API an agent connects to a new entry point.
Now leveraged by autonomous workflows with no human in the loop.
Enterprises can’t see every action behind the connections and workflows.

Sensitive data is moving through AI interactions none of your existing controls were designed to see.

M&A terms in a prompt. HR records surfaced in a response.
IP walking out through an AI tool nobody approved.
It is happening now, not in the future.

This is not a future problem. It is happening now.

Current AI Trends

SECUR-SERV + proofpoint

Email Management by AI is one of the most common applications for employed Americans

Source: Gallup- Oraganization AI Update

Poll Question #3

How many phishing emails have you encountered in the last year?

- None
- 1-5
- 6-10
- Too many to count

SECUR-SERV
+
proofpoint.

5 Things About Cybersecurity That May Not Be True Anymore

Assumption #1

Microsoft 365 Gives Us All the Email Protection We Need.

SECUR-SERV + proofpoint

The Assumption

Microsoft 365 keeps our email environment safe.

Today's Reality

- Advanced impersonations
- Business email compromise
- Evolving phishing techniques
- Human-targeted attacks
- Limited visibility without additional threat intelligence

27%

of advanced threats are not detected by Microsoft

$26/mo

is how much it costs an attacker to test Microsoft's defenses

The Shift: Email security now requires defense in depth.

Assumption #2
Phishing Emails Are Easy to Spot.

SECUR-SERV + proofpoint

The Assumption

Phishing emails are easy to identify by common red flags.

Today's Reality

- Localization
- Personalization
- Executive impersonation
- Scale
- Research

The Shift: A well-written email is no longer a sign that it's legitimate.

Assumption #2
Phishing Emails Are Easy to Spot.

SECUR-SERV + proofpoint

Example Profile on one of the authors

Interests

Based on the profile of [the author], it is highly likely that [the author] is deeply interested in the intricacies of artificial intelligence, particularly in areas concerning AI safety and alignment. [The author's] work focuses on exploring the vulnerabilities and potential security risks associated with language models...

Professional Profile

...

Academic Profile

... [the author] has co-authored a paper titled [removed] which examines ...

Colleagues

Worked with: - [removed] (found on [the author's] personal website)

...

Example email: AI-generated

Subject: Research collaboration on AI threat modeling

Hi [Name],

Your recent paper on LLMs and phishing detection caught my attention. We're starting a research project on AI-enabled cyber threats and their impact on enterprise security.

Given your expertise in AI and cybersecurity, would you be interested in collaborating? You can review the project details and apply here: View Project Details.

Application deadline: November 18, 2024.

Best,
James Chen
Research Coordinator

Assumption #3

If There's No Malicious Link or Attachment, We're Safe.

SECUR-SERV + proofpoint

The Assumption

If there's no malicious link or attachment, the email is safe.

Today's Reality

- Business email compromise
- Wire fraud
- Gift card fraud
- Payroll diversion
- Vendor fraud
- Conversation attacks

The Shift: The payload isn't always malware. Sometimes it's trust.

Assumption #4

If the Email Came From a Real Account, It's Legitimate.

SECUR-SERV + proofpoint

The Assumption

Emails from real people and trusted accounts can be trusted.

Today's Reality

- Account takeover
- Compromised suppliers
- Partner compromise
- Thread hijacking
- Internal account compromise

The Shift: Trusted identities can become attack infrastructure.

Assumption #5
Cybersecurity Is Primarily an IT Problem

SECUR-SERV + proofpoint

The Assumption

Cybersecurity is an IT problem.

Today's Reality

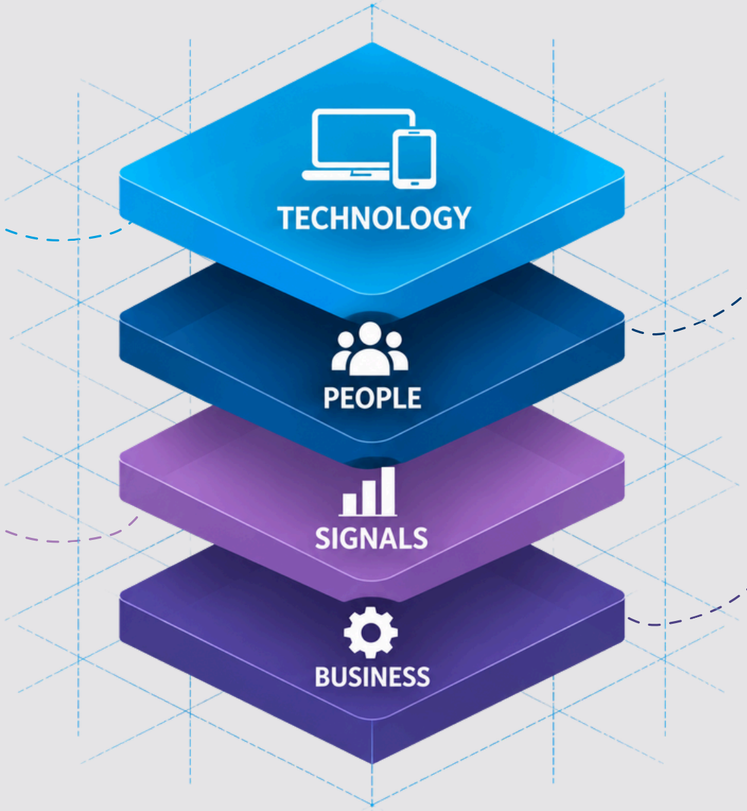
The Shift: Cybersecurity becomes a business-risk issue, not simply a technology issue.

The Modern Cybersecurity Blueprint

SECUR-SERV + proofpoint

Protect the Technology
Email + Endpoint + Identity

Connect the Signals
Threat intelligence + Analytics + AI



Protect the People
Security awareness + Behavioral insights

Prepare the Business
Processes + Verification + Incident response

Cybersecurity has changed. Has yours?

SECUR-SERV
+
proofpoint.

From Theory to Reality

From Theory to Reality

Real-world examples of email threats in action.

SECUR-SERV + proofpoint

Scenario 1: Business Email Compromise (BEC)

A threat actor impersonated the CEO using a lookalike **.co** domain instead of **.com** and sent the Controller an urgent, confidential wire transfer request. The email appeared authentic, including the CEO's real signature, and resulted in a **~$300,000 fraudulent transfer.**

Scenario 2: Malicious Email Attachment

An employee at a healthcare company received a spoofed vendor email with a **malicious invoice attachment**. Opening the file introduced malware that spread across the network, **exposed sensitive patient data, encrypted systems, and ultimately led to a ransom demand.**

Poll Question #4

What is your biggest cybersecurity concern right now?

- Agentic AI and emerging AI risks
- Data leakage and data protection
- Identity and account compromise
- Internal threats

SECUR-SERV + proofpoint.

Open Q&A

Have a question or a scenario? Drop them in the chat.

SECUR-SERV
+
proofpoint.

Defense & Best Practices

A ONE-PAGE EMAIL RISK SNAPSHOT.

Email Security Validation Review

SECUR-SERV + proofpoint

You already have controls; let's pressure-test whether they're doing what you think they're doing.

Potential Risk Areas	What We Check
1 What's getting through?	Phishing, BEC, impersonation and malicious messages their current defenses aren't stopping
2 Can your identity be abused?	MFA strength, suspicious forwarding, mailbox/account takeover exposure
3 Can someone impersonate you?	SPF, DKIM, DMARC, domain spoofing and lookalike exposure
4 Who is most exposed?	Executives, finance/AP, HR and other highly targeted employees
5 What happens after the click?	Reporting, investigation, containment and response process

Request Your Email Security Validation Review

SECUR-SERV + proofpoint.

Take the next step toward stronger email security.

Phone 800-228-3628

Website secur-serv.com