AMPLIFY

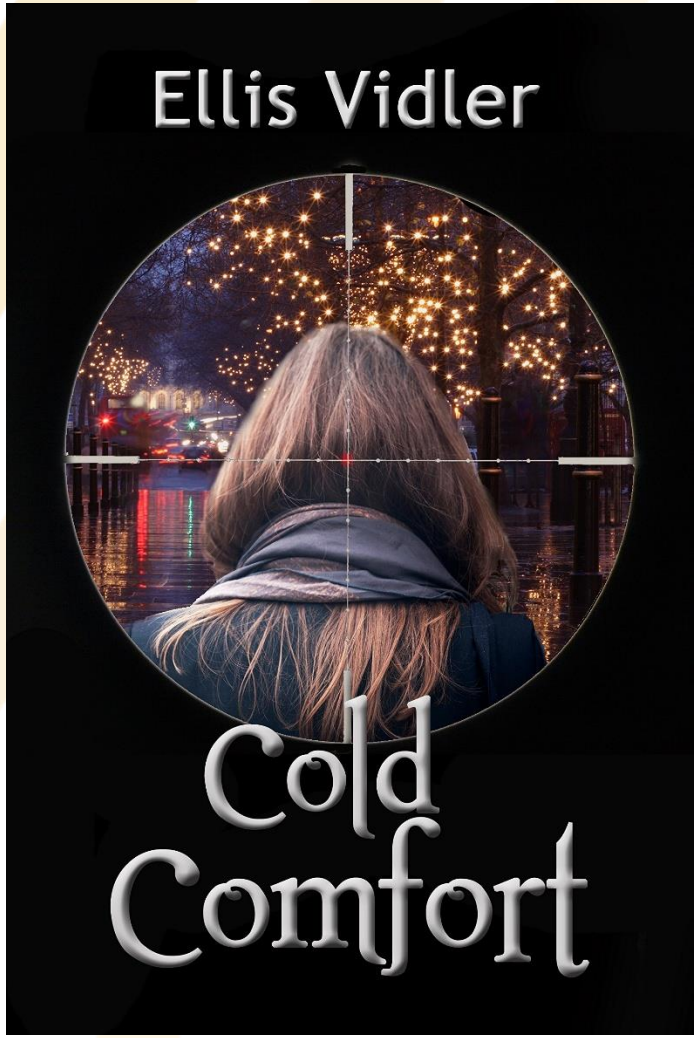
Tech Wrecks: Tales of Tech Gone Sideways

Patrick Kelly, President 4th Season Consulting

“Bad decisions…

…make good stories.”

-- Ellis Vidler



Introduction

Patrick Kelly

President, 4th Season Consulting

Financial Disclosures

4th Season Consulting Owner

“You must learn from the mistakes of others. You can’t possibly live long enough to make them all yourself.”

-- Sam Levenson

Common Causes

Cyber Attacks

Human Error

Outdated Systems

Infrastructure Failure

3rd Party Risks

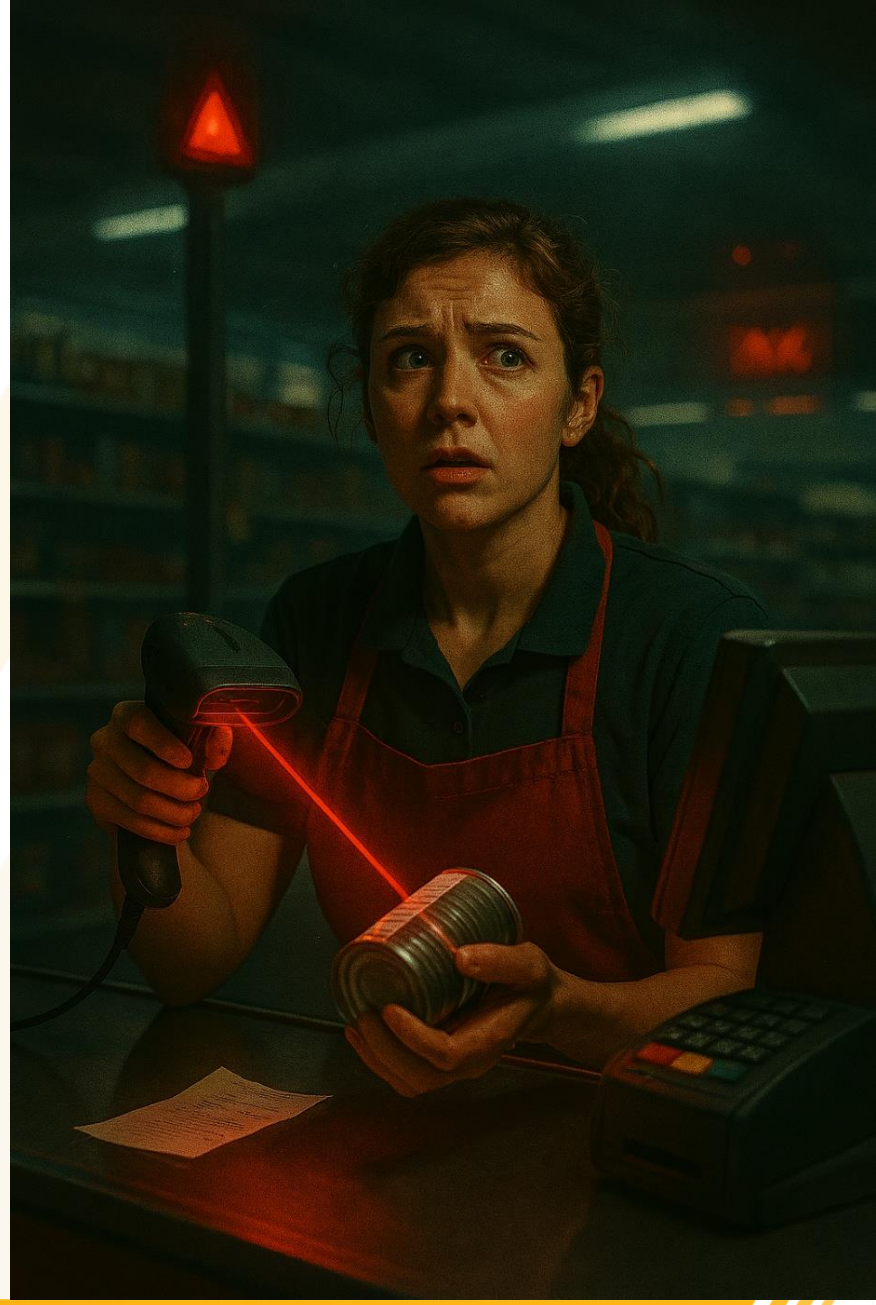
“Companies spend millions of dollars on firewalls, encryption, and secure access devices and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer, operate and account for computer systems that contain protected information.”

-- Kevin Mitnick

(Hackerous Extraordinous)

The Silence of the Scans

- $1 Million/Week Grocery Store
- Thanksgiving Week
- Historically Difficult Store Director
- Young Support Staff Trying to be Proactive



Mission: Impossible – Password Protocol

- Practice with Two Locations
- COO Walked Out
- Held Access for Ransom
- Improperly Changed Website

Gone with the Upgrade

- Mom and Pop Recruiting Company
- Upgrade QuickBooks
- Overwrote QuickBooks Data
- No Backups
- 15 Years of Accounting History

The Fast and the Frivolous

- Point of Sale Company
- Credit Card Processing Feature
- Developer Used his CC for Testing
- Code Moved to Production

“You cannot learn to swim by reading a book. You have to get into the water.

-- Shiv Khera

Cyber Attacks

Ransomware
Distributed Denial of Service (DDoS)
SQL Injections
Brute Force Attacks

Phishing

Who	Anthem (2014-2015)
What Happened	Email sent to small group of employees One employee followed link Fake page to harvest credentials 80 million records stolen
Impact	$115 million class action settlement $16 million HIPAA settlement $40 million state attorneys general settlement $260 million on security upgrades and response
Prevention	Training Minimal necessary credentials Multi-factor authentication

Human Error

Default Credentials
Theft
Developer Error
Plain Text Passwords
Unsecured Communications
Hardcoded Credentials
Shadow IT

Misconfiguration

Who	University of Washington (UW) Medicine (2018)
What Happened	Web server hosting an accounting of disclosures database accidentally configured to allow public access, exposing 974,000 patients' data to be indexed by search engines
Impact	UW paid $750,000 related to HIPAA issues Class action lawsuit
Prevention	Change control process QA Training Data segmentation Automated configuration management

Outdated Systems

Unapplied OS Updates
Outdated OS
Old Software
Unsupported Hardware

Missed Patches

Who	Equifax Data Breach (2017)
What Happened	Failed to patch a known flaw in Apache Struts, allowing attackers to steal data from 147 million people, exposing critical personal information including Social Security numbers and birthdates
Impact	$700 million FTC, CFPB, and states settlement $1.4 billion in security upgrades/legal fees CEO, CIO, and CSO resigned
Prevention	Patch management process Automated vulnerability scanning Audits of critical systems

Infrastructure Failure

Power Outage
Hardware Failure
Spills and Drops
Cooling Systems

Network Outage

Who	FAA Air Traffic Control Outage (2025)
What Happened	Contractor accidentally severed two critical fiber optic cables, knocking out both primary and backup systems at the FAA's Dallas TRACON facility
Impact	Over 1,000 flights delayed or canceled 100,000+ travelers affected American could depart 9 planes in 3 hours
Prevention	Redundant systems Capacity planning Disaster recovery drills

Third Party Risks

Inadequate Network Segmentation
Vulnerable Infrastructure
Lack of Security
Vendors of Vendors

Access Management

Who	Target Data Breach (2013)
What Happened	Hackers accessed Target's network using stolen credentials from an HVAC contractor, then moved laterally to install malware on point-of-sale terminals and steal customer payment data
Impact	$290 million estimated costs CEO and CIO resigned 50% drop in Q4 2013 profits 9% decline in stock price within two months
Prevention	Multi-factor authentication Principle of least privilege accounts Network segregation

Anatomy of a Phish

Spoofed Domain

Urgent Deadline

Dire Consequences

From: IT Support <it-support@we11point.com>
Subject: Urgent: Security Update Required
Date: December 12, 2014
To: Patrick Kelly

Patrick,

As part of our ongoing security enhancements, all employees are required to verify their credentials to avoid service disruption.

Please click the link below to complete the verification process in the next 24 hours:

Verify Now

Failure to comply will result in suspension of access to internal systems.

IT Security Team
WellPoint Inc.

Password Hygiene

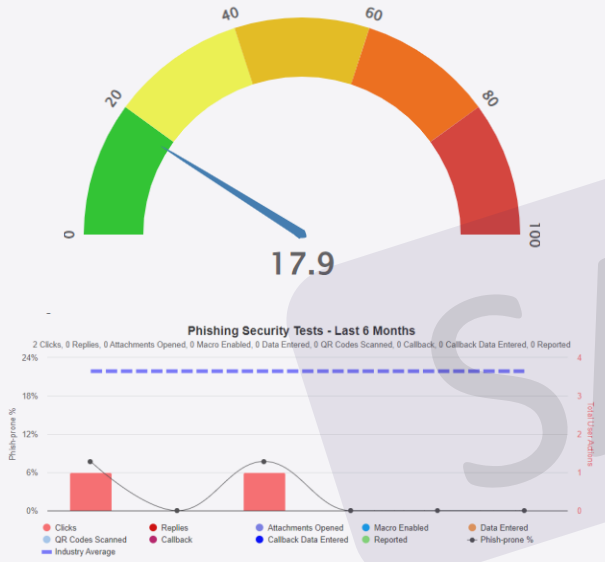
"Passwords are like underwear.
You should change them often.
Don't share them.
Don't leave them out for others to see.
Oh, and they should be sexy, I mean they should be mysterious."
-- **Eric Griffin (PC Online)**

Length: Aim for at least 12–16 characters
Complexity: Use a mix of letters, numbers, and symbols
Unpredictability: Avoid names, birthdays, or common phrases
Uniqueness: Never reuse passwords across accounts
Storage: Use a password manager to keep track securely

Scorecards and KPIs

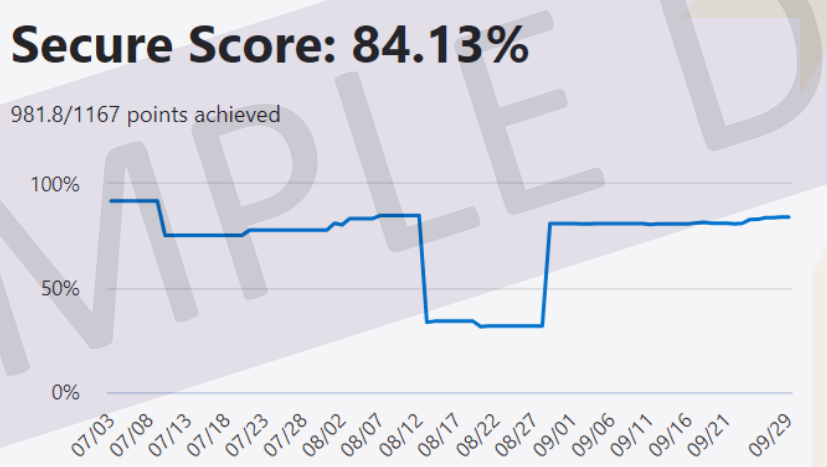
Phishing

Monthly phishing campaigns with training



Policies

Overall environment score based on policies

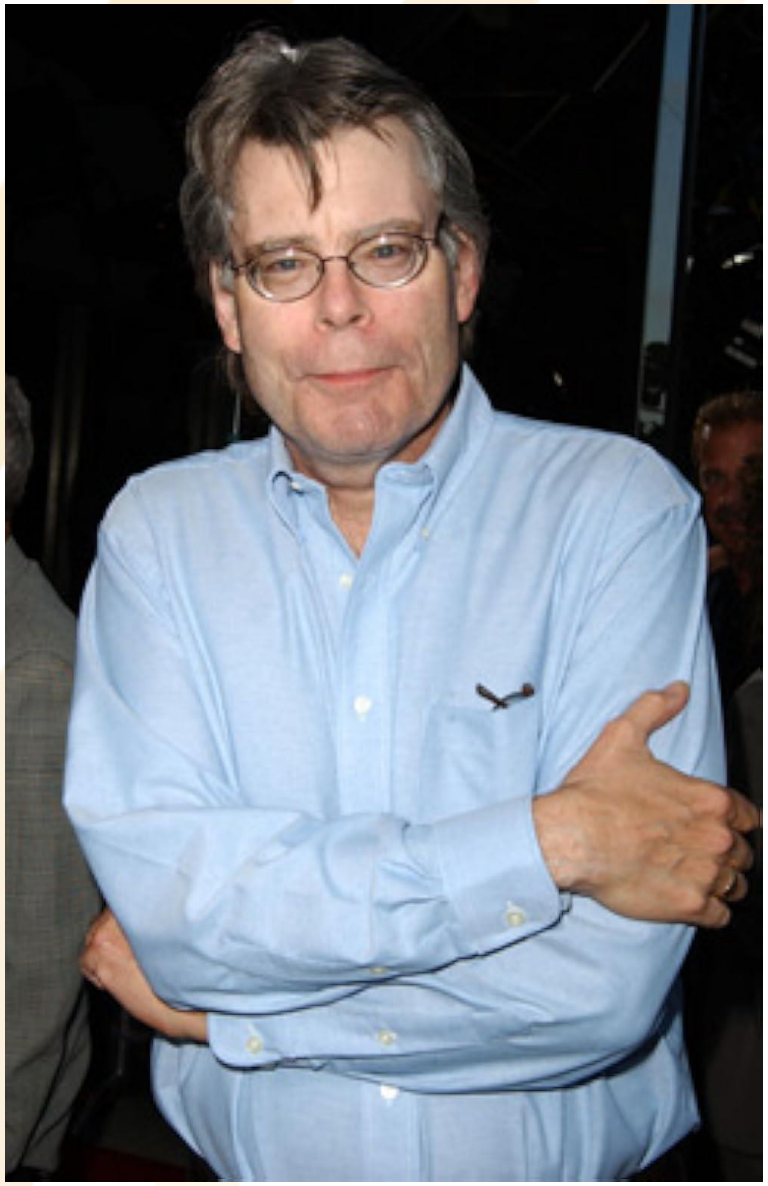


Endpoint

Specific endpoint recommendations

“The trust of the innocent is the liar's most useful tool.”

-- Stephen King



Vishing Video in Real-Time

Garrett Myler

Final Thoughts

- Bad things happen to all sized organizations
- If you are not measuring it, you are not managing it
- Backups are like insurance - once you realize you need it, it’s too late
- Good security need not be expensive security
- The best silicon-based security is only as good as your least-trained carbon-based asset

I Need Your Feedback – Scan the QR

Prefer paper?

On the form in front of you, please score me and the content I shared with you today.