DefenseStorm®

STEVE SOUKUP
Chief Revenue Officer
DefenseStorm

PREPARING FOR NEXT-GEN CYBER ATTACKS

How Credit Unions Can Stay Ahead of Cyber Bad Actors

AGENDA

THE PROBLEM

THE DAMAGE

PRACTICAL NEXT STEPS

WHAT ARE THE ODDS?

1 in 292,000,000

WHAT ARE THE ODDS?

1 in 292,000,000

1 in 1,000,000

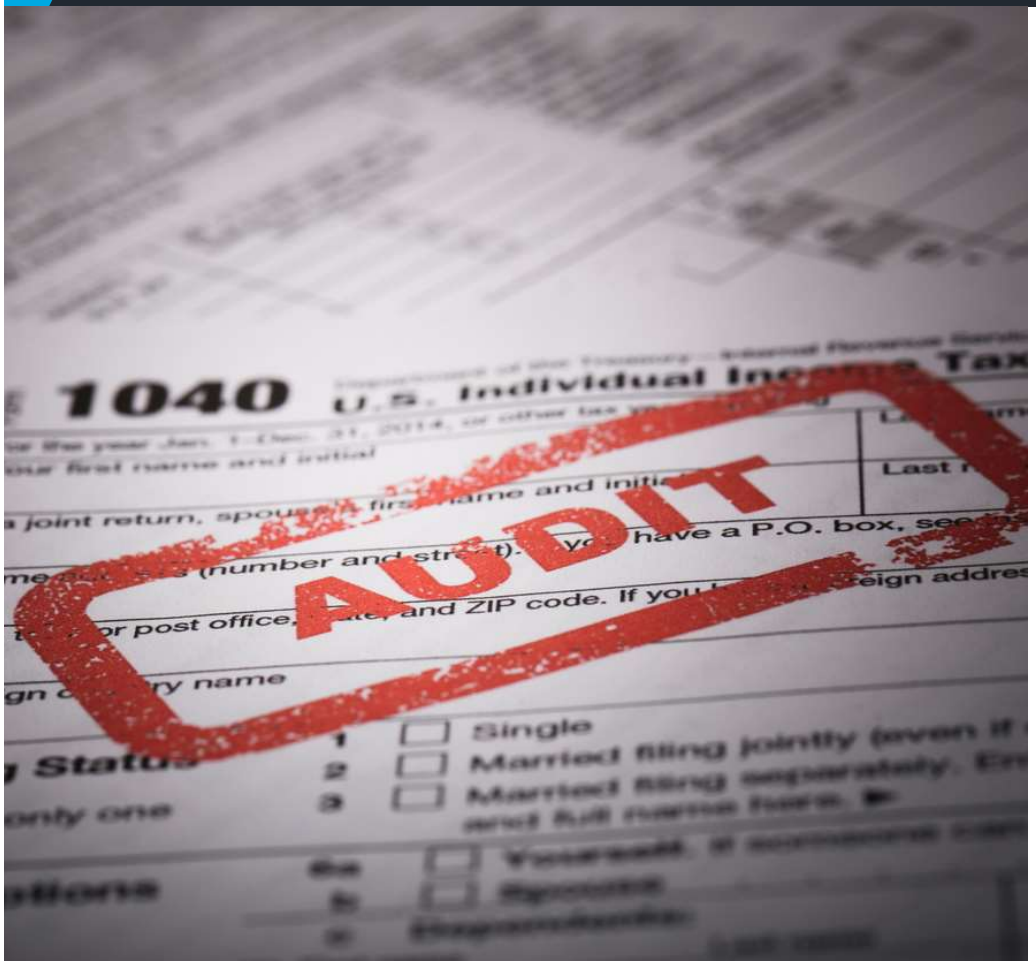
WHAT ARE THE ODDS?

1 in 292,000,000

1 in 1,000,000

1 in 12,000

WHAT ARE THE ODDS?



1 in 292,000,000

1 in 1,000,000

1 in 12,000

1 in 160

WHAT ARE THE ODDS?

1 in 292,000,000

1 in 1,000,000

1 in 12,000

1 in 160

1 in 4

THE BIG HURT

IS ON FOR COMMUNITY FIs

50%

Cyber breach increase

3M GAP

Cyber staff shortages

#1 FED FOCUS

Regulatory pressures

THE THREAT…

The release of sensitive, protected or confidential information to an untrusted environment.

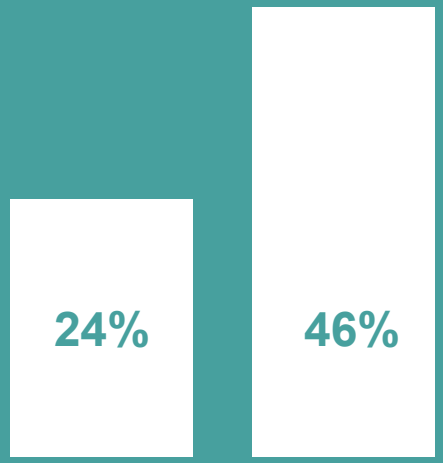
Intentional or unintentional

Outside attack or inside actors

Data is copied, transmitted, viewed, stolen or used by someone unauthorized to do so

IS GROWING…

The number of organizations reporting a breach “in the last year” nearly doubled year over year.



… AND GROWING

It takes 9+ months to identify and resolve breaches.

191
DAYS TO IDENTIFY

+

66
DAYS TO RESOLVE

=

257
DAYS TO IDENTIFY

THE CYBERSECURITY TALENT SHORTAGE JUST MAKES THINGS WORSE

THE COSTS ARE RISING

$233 Cost /breached record **x** **10,000** Records **=** **$2.3M**

20M

Cyber events per day per FI

*DefenseStorm average

200K

Cyber alerts per day per FI

*American Banker research average

2 hour

Regulators' recovery time expectation

*FFIEC official

Keeping community banks and credit unions secure from data breaches requires a different approach

- Credit unions are held to a higher regulatory standard
- Multiple tools & manual processes = complexity & resource intensiveness
- People are the weakest link AND the strongest defense

YOU CAN'T BE CYBERSECURE WITHOUT BEING **CYBERCOMPLIANT**

3 CULTURE OF CYBERSECURITY COMPLIANCE DRIVERS

How do we know we're doing the **right** things?

How do we know we're doing the **right** things **right**?

How do we ***prove*** we're doing the **right** things **right**?

WHAT LEVEL OF EXPOSURE CAN YOU TOLERATE?

Co-managed, combined cybersecurity and cybercompliance delivers real time cyber safety and soundness

BANKING FOCUSED IN-HOUSE BUILD

- Build it yourself
- Best of breed solution
- Best of breed talent
- In-house specialist talent (certified)

OUTSOURCED

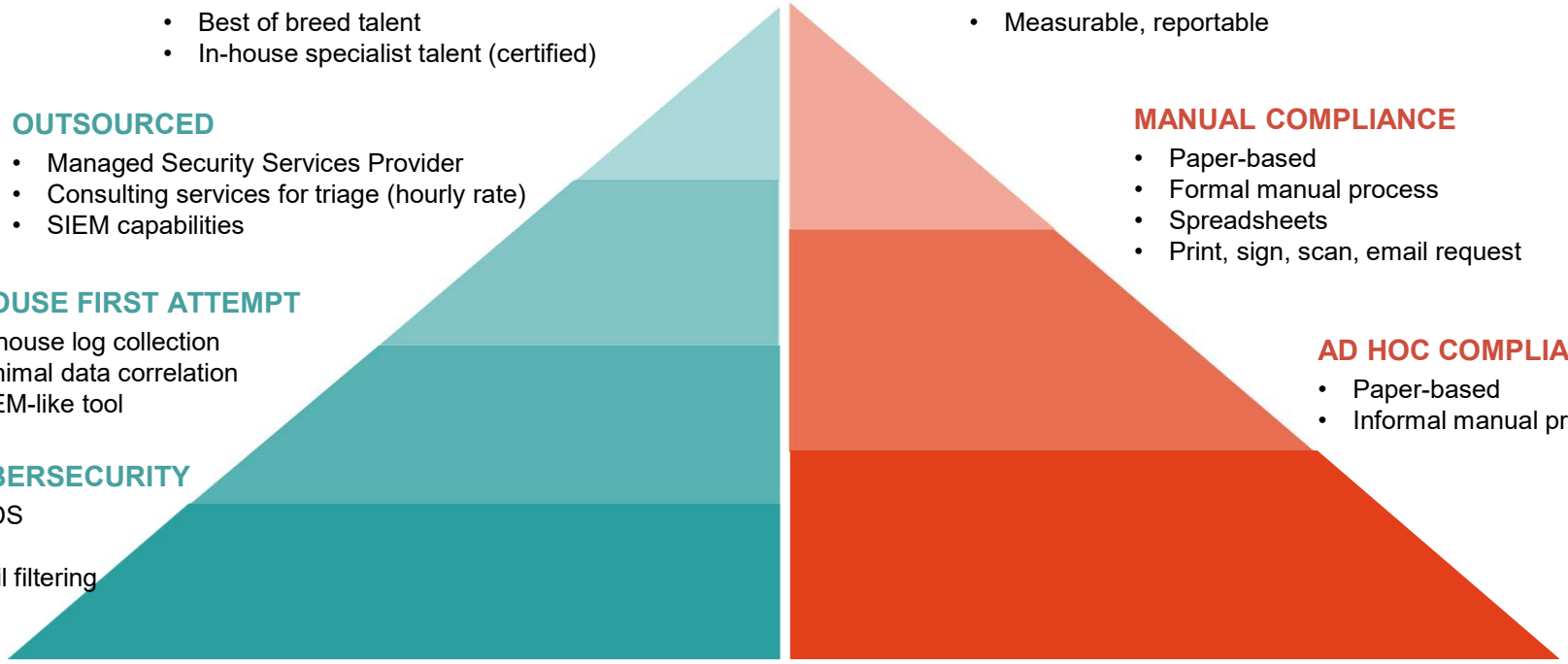
- Managed Security Services Provider
- Consulting services for triage (hourly rate)
- SIEM capabilities

IN-HOUSE FIRST ATTEMPT

- In-house log collection
- Minimal data correlation
- SIEM-like tool

BASIC CYBERSECURITY

- Firewall/IDS
- Anti-virus
- Web/email filtering



AUTOMATED STANDALONE COMPLIANCE

- Digitized formal process
- Task driven
- Measurable, reportable

MANUAL COMPLIANCE

- Paper-based
- Formal manual process
- Spreadsheets
- Print, sign, scan, email request

AD HOC COMPLIANCE

- Paper-based
- Informal manual process

CYBERSECURITY EXPOSURE SCALE

CYBERCOMPLIANCE EXPOSURE SCALE

Gartner

*"**A revolution is coming…**that will sweep away many security products and replace them with **"product-service fusions"** where you pay one amount for using the tools together with ongoing help with their operation."*

– ANTON CHUVAKIN
IS SECURITY JUST TOO DAMN HARD? IS PRODUCT+SERVICE THE FUTURE?

THE KEY: MAP CYBERSECURITY DATA TO NCUA ACET AND YOUR CREDIT UNION POLICIES

DRIVER 1

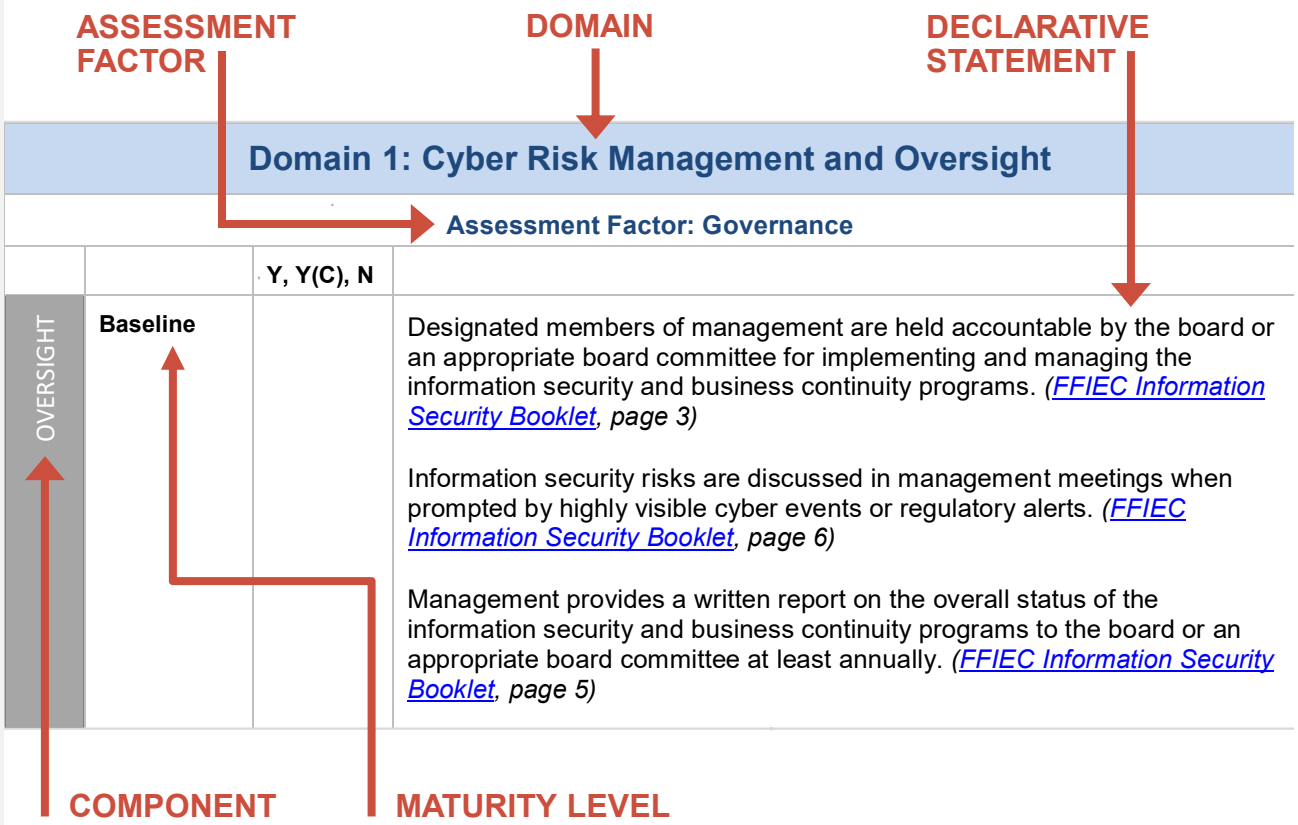
How do we know we're doing the **right** things?

DRIVER 2

How do we know we're doing the **right** things **right**?

DRIVER 3

How do we ***prove*** we're doing the **right** things **right**?




SO WHAT DO
YOU DO NEXT?

GET YOUR BOARD OF DIRECTORS INVOLVED

1. Help establish vision, risk appetite & strategic direction
2. Review management & third-party analysis of maturity level
3. Review findings about how cybersecurity preparedness aligns with risks
4. Review & approve plans to address risk management & control weaknesses
5. Review the results of management's ongoing monitoring of exposure to and preparedness for cyber threats

ESTABLISH WRITTEN POLICIES & CONTROLS

These become a living, breathing part of your **security and compliance culture**

CHOOSE A SOLUTION THAT SUPPORTS ALL 3 DRIVERS

DRIVER 1

How do we know we're doing the **right** things?

DRIVER 2

How do we know we're doing the **right** things **right**?

DRIVER 3

How do we ***prove*** we're doing the **right** things **right**?

WHAT TO LOOK FOR

Metrics based on industry-specific framework

- FFIEC CAT, ACET
- CIS Critical Security Controls

Analyze & prioritize findings

Risk treatment methodology

Forensic-style evidence of vulnerability or exploit

WHAT TO LOOK OUT FOR

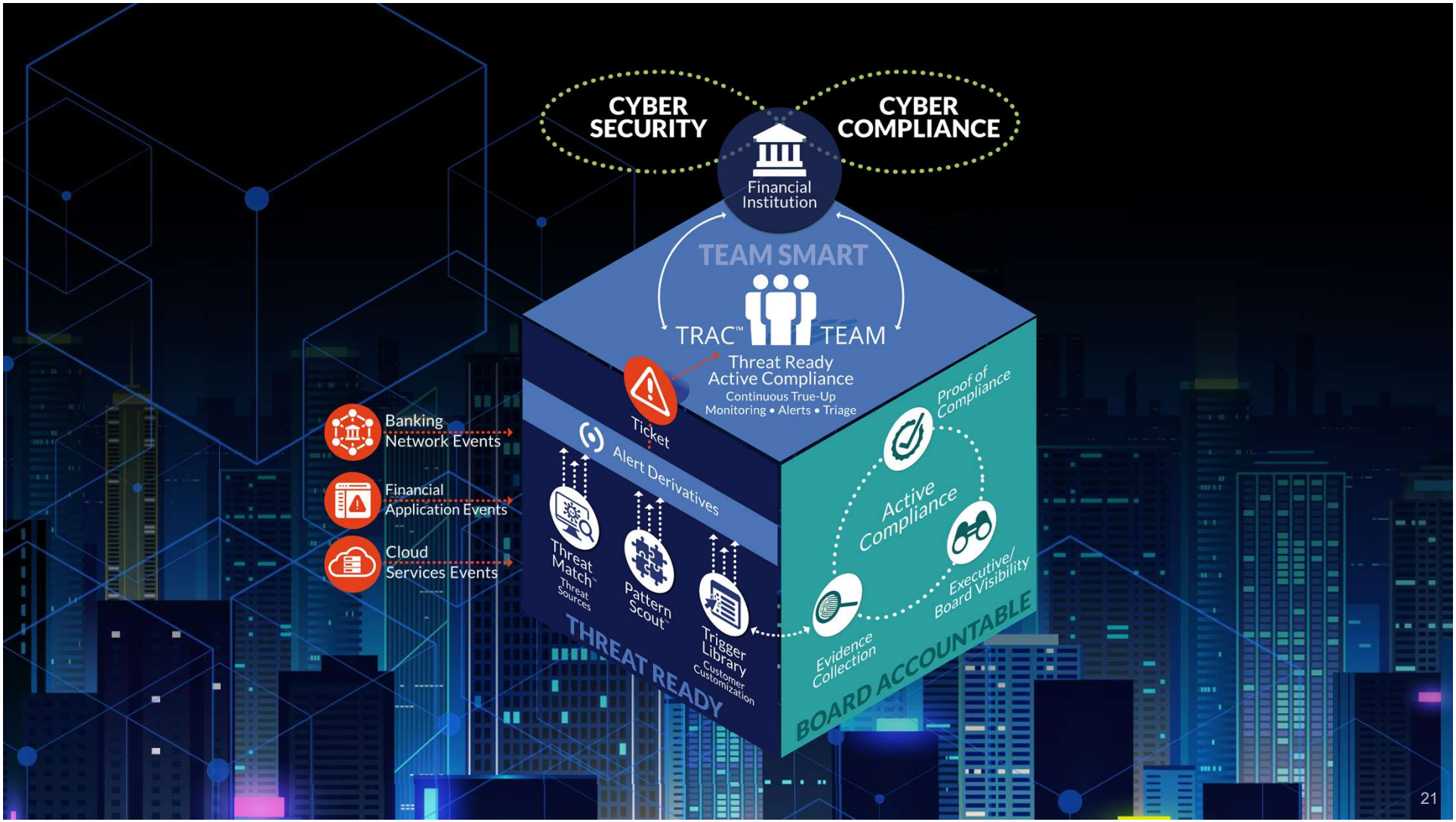
Fat report = better (it's not)

Endless lists of vulnerabilities

Patch-all mindset without priorities

No clear strategy for risk treatment

60+ pages of glossary


CYBER SECURITY
CYBER COMPLIANCE
Financial Institution
TEAM SMART
TRAC™ TEAM
Threat Ready Active Compliance
Continuous True-Up
Monitoring • Alerts • Triage
Ticket
Alert Derivatives
Banking Network Events
Financial Application Events
Cloud Services Events
Threat Match™
Threat Sources
Pattern Scout™
Trigger Library
Customer Customization
THREAT READY
Proof of Compliance
Active Compliance
Executive/ Board Visibility
Evidence Collection
BOARD ACCOUNTABLE

*"We couldn't do in days what **DefenseStorm does for us in minutes**. The benefits of being able to satisfy our examiners & auditors when they ask us questions, and being able to feed that back to the Board, **that's the ROI**."*

– CARLOS VAZQUEZ, VP OF INFORMATION TECHNOLOGY

DefenseStorm®

QUESTIONS AND ANSWERS

STEVE SOUKUP

Chief Revenue Officer

DefenseStorm

@StephenSoukup

Steve.Soukup@DefenseStorm.com

440.670.8567