



Implementing Security Controls within a School
Network

A decorative graphic consisting of several overlapping orange arrows pointing to the right, located in the top-left corner of the slide.

Agenda

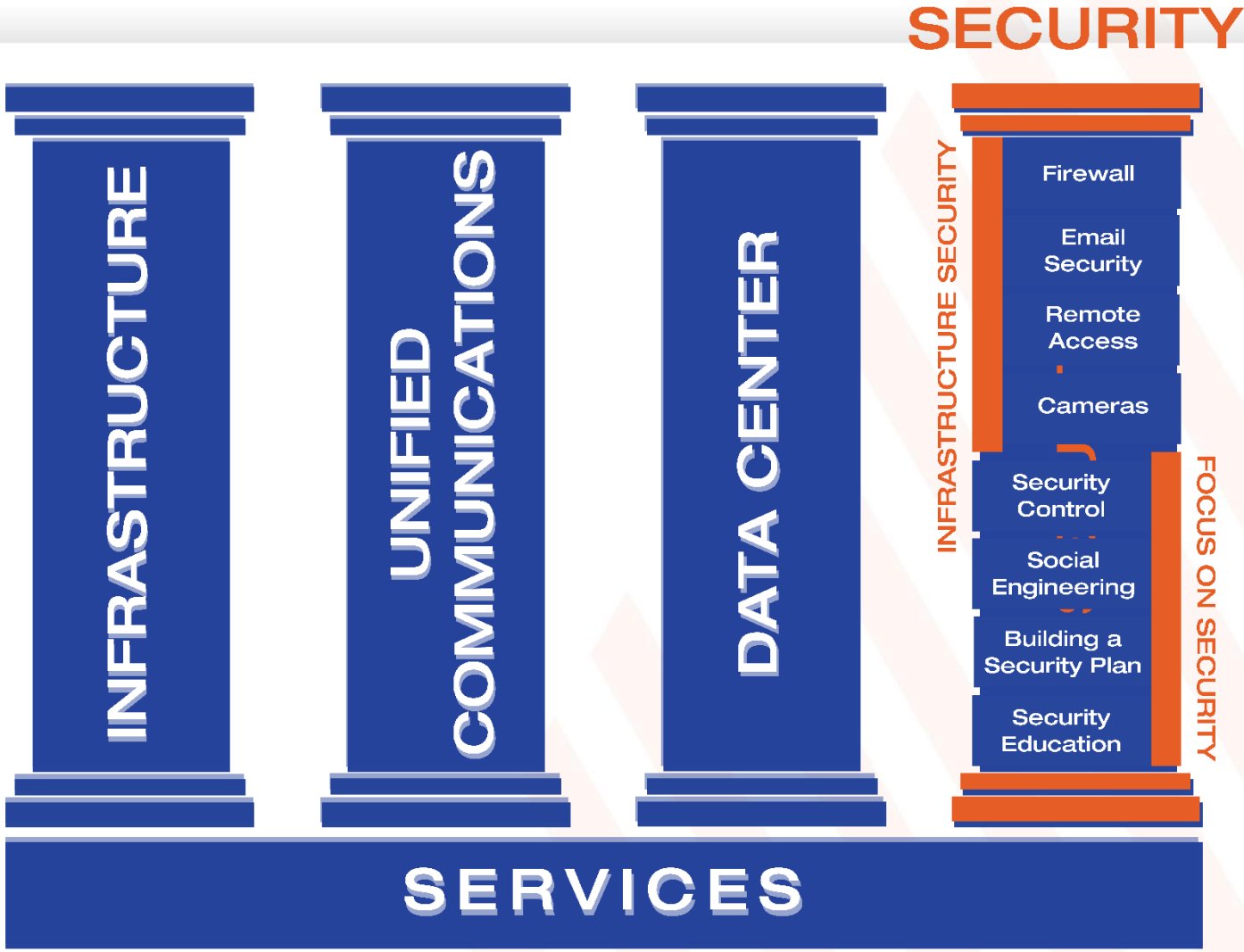
- Introduction
- State of Security
- Security Controls
 - Prioritizing assets
 - Identifying what is on controlled network
 - Managing software on controlled network
 - Segmenting networks
 - Patching plans
 - Administrative access
 - Secure configurations

Who is High Point Networks

- Founded in 2003
- Corporate office in West Fargo, ND
- Locations:
 - Offices
 - Bismarck (ND), Billings (MT), Sioux Falls (SD), Detroit Lakes (MN), Brookings (SD), Minneapolis (MN), Denver (CO), Pueblo (CO)
- 134 Employees Today



Our Core Business Solutions



A decorative orange arrow pointing right, located in the top left corner of the slide.


My Background

- 9+ years as a Network Engineer at High Point Networks
 - Focused on routers, switches, wireless and firewalls
- Prior to that, spent six years as a Network Administrator
- Ran HPN's managed services for five years
- Security team lead for HPN for two years
- Currently Director of Internal IT for two years

State of Security

A decorative orange arrow pointing right, located in the top left corner of the slide.

Users are the biggest security threat

- No technology or software available will block every threat, so we need to rely on users
 - Since we can't rely on users wholly, we need to look at ways to mitigate as many threats as possible
- 
- A series of diagonal, light pink lines that create a sense of movement and depth in the bottom right corner of the slide.

Hackers steal \$800,000

Hackers steal \$800,000 from Cape Cod Community College



CAPE COD COMMUNITY COLLEGE/FILE

Hackers stole more than \$800,000 from Cape Cod Community College last week when they infiltrated the school's bank accounts, the school notified its employees Friday.

Data breach affecting 2000 people



AOS #77 Sunrise County School System

P.O. Box 190 – 100 High Street

Eastport, Maine 04631

Ph: 207-853-2567 – Fax: 207-853-6260

Alexander – Baring Plt. – Charlotte – Crawford – Dennysville – Eastport – Lubec – Pembroke – Perry

Friday, December 7, 2018

To Whom It May Concern,

I regret to inform you that the Central Office has experienced a data breach by an unknown entity that has put some information at risk of being compromised.

More specifically, the type of information that could potentially be at risk would include name, date of birth, physical and mailing address and unfortunately, direct deposit numbers, as well as social security numbers. This information is kept in the Central Office since it was/is related to your employment with a school department in our district. This includes employment with former districts such as School Union 104, School Union 106, MSAD 19/RSU 85 and currently AOS 77.

Other personal information, such as credit card numbers, would not be affected since we do not have that type of information.

As a precaution, I encourage you to closely monitor your financial transactions and watch for anything that may be an anomaly. Whatever financial institution you conduct business with has their own security measures and I am sure they could answer some questions for you as well.

2019 Trends – Computing Power

Cyberthreats in 2019: The Trends That Will Continue to Move Upward



By [Ryan Olson](#)

December 12, 2018 at 6:00 AM

Category: [Unit 42](#)

Tags: [2019](#), [Cryptocurrency](#), [email compromise](#)

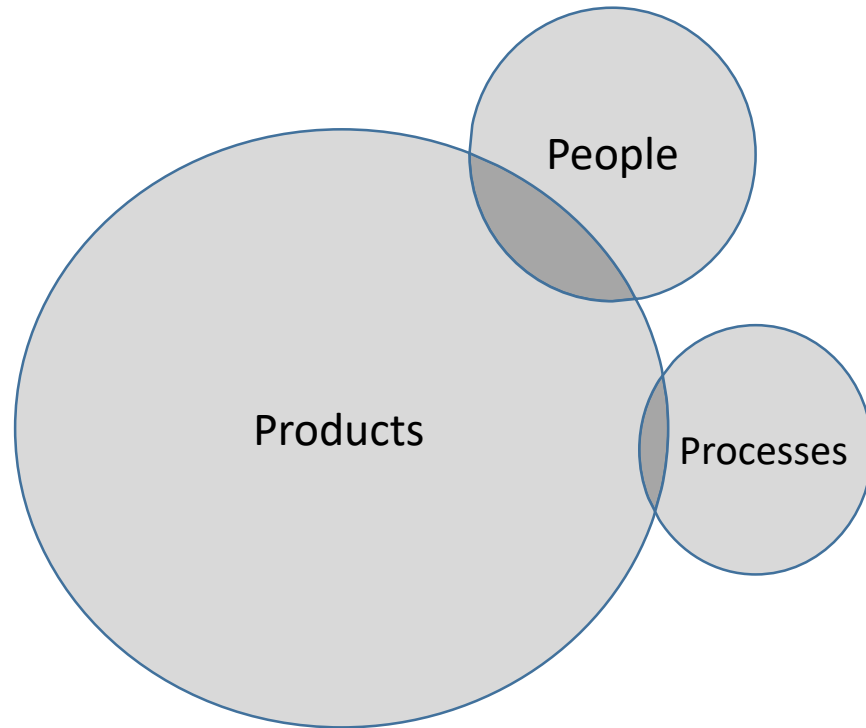
When it comes to realistic predictions for the year ahead, my philosophy is simple: there are certain trends that research shows will continue to move upward. With that said, in 2019, I believe we are going to see:

1. More Attacks With the Eventual Goal of Cryptocurrency Mining

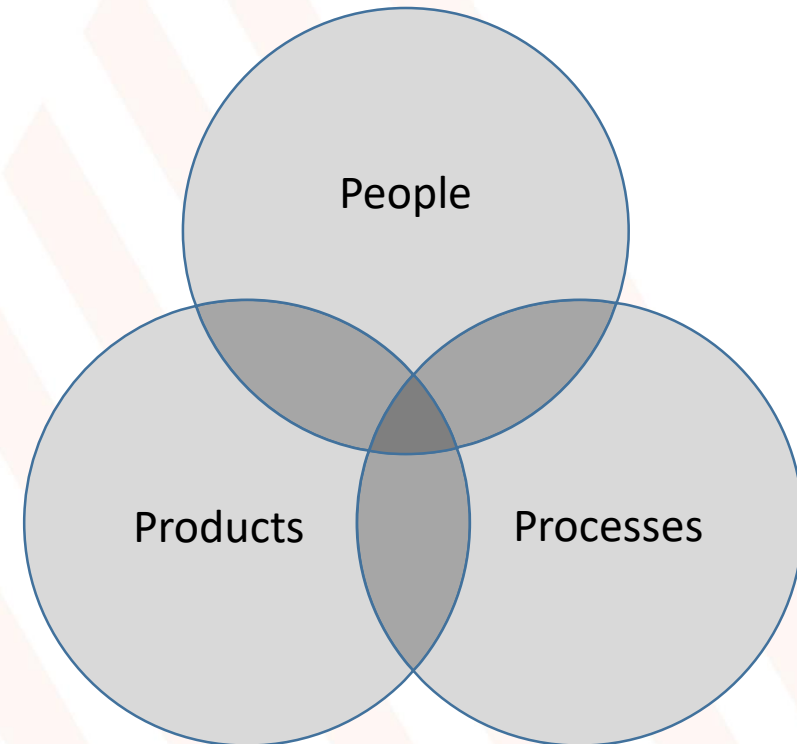
We saw a huge uptick in this at the end of last year that [continued throughout 2018](#). Cryptocurrency mining is the process through which currencies like bitcoin are created. The “mining” process involves racing to perform a series of calculations to solve a cryptographic problem. The person who wins the race is awarded a block of coins, and the more CPU power someone can throw at those calculations, the better their chance at winning. It has become too safe a way for attackers to make money. Although I don’t predict this will skyrocket, I do see it being a continuous point in the threat landscape of which people and businesses alike need to be aware.

Security Controls

Fixing Security?



We are seeking a magic product that will fix security



Solving security takes a combination of all three

Process – When can money be transferred?

School district fails to reclaim \$120,000 wired by bank to scammer

© 2 months ago 4 Min Read



A school district in Indiana which had \$120,000 transferred from its bank account after its email account was hacked, has failed in an attempt to reclaim the cash.

The problems for Lake Ridge Schools began in October 12 2016 when money earmarked for part of a seven million dollar construction project of an athletics complex at Calumet New Tech High School was fraudulently wired to parties unknown.

A decorative orange arrow pointing to the right, located on the left side of the slide.

Process – How do we verify the plan?

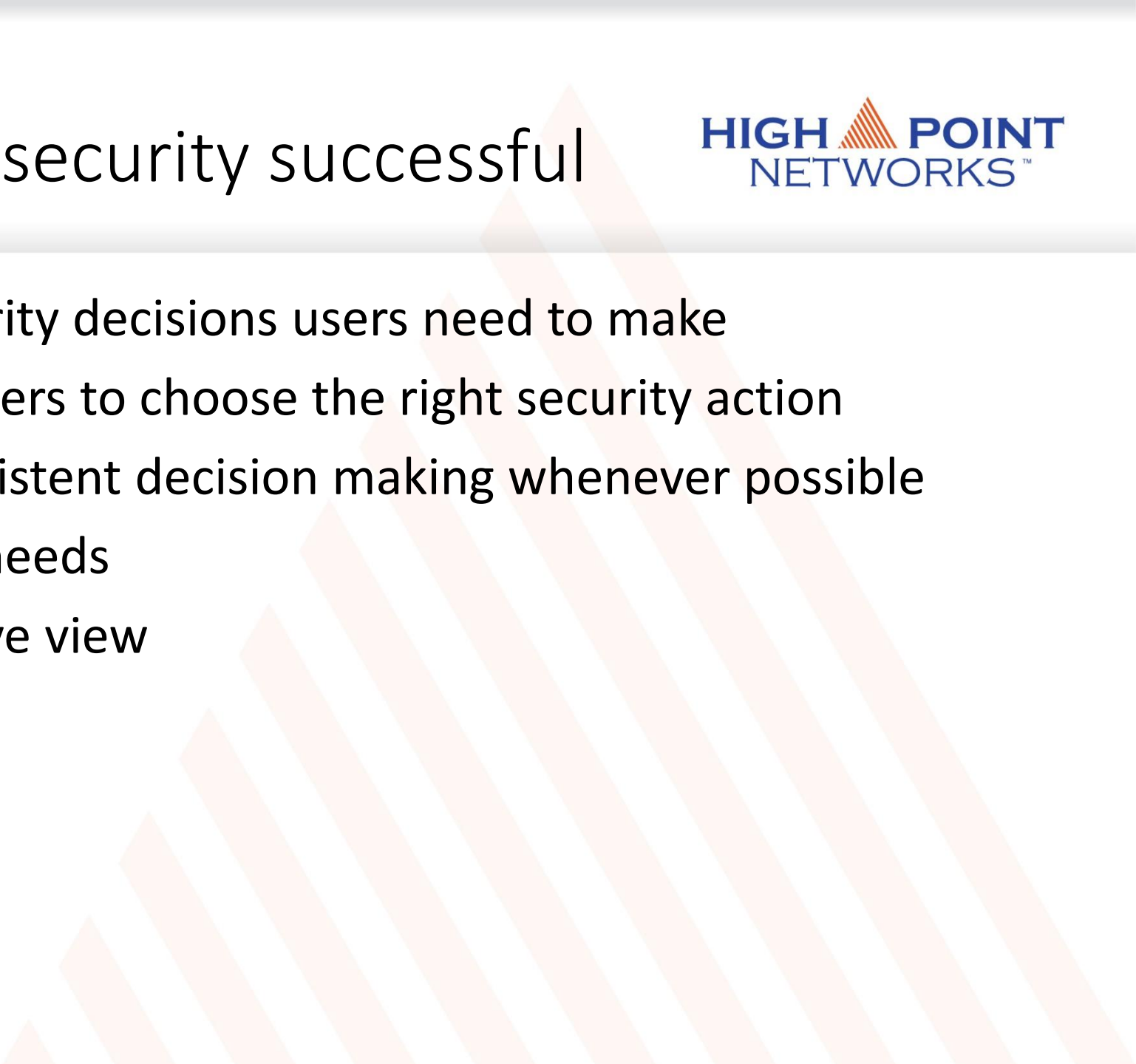
Mandan High School accidentally leaks student information



MANDAN, N.D. — A central North Dakota high school leaked more than a thousand students' information, including lunch pin numbers and locker combinations, in a mass email the school said it accidentally sent on Monday, Jan. 7.

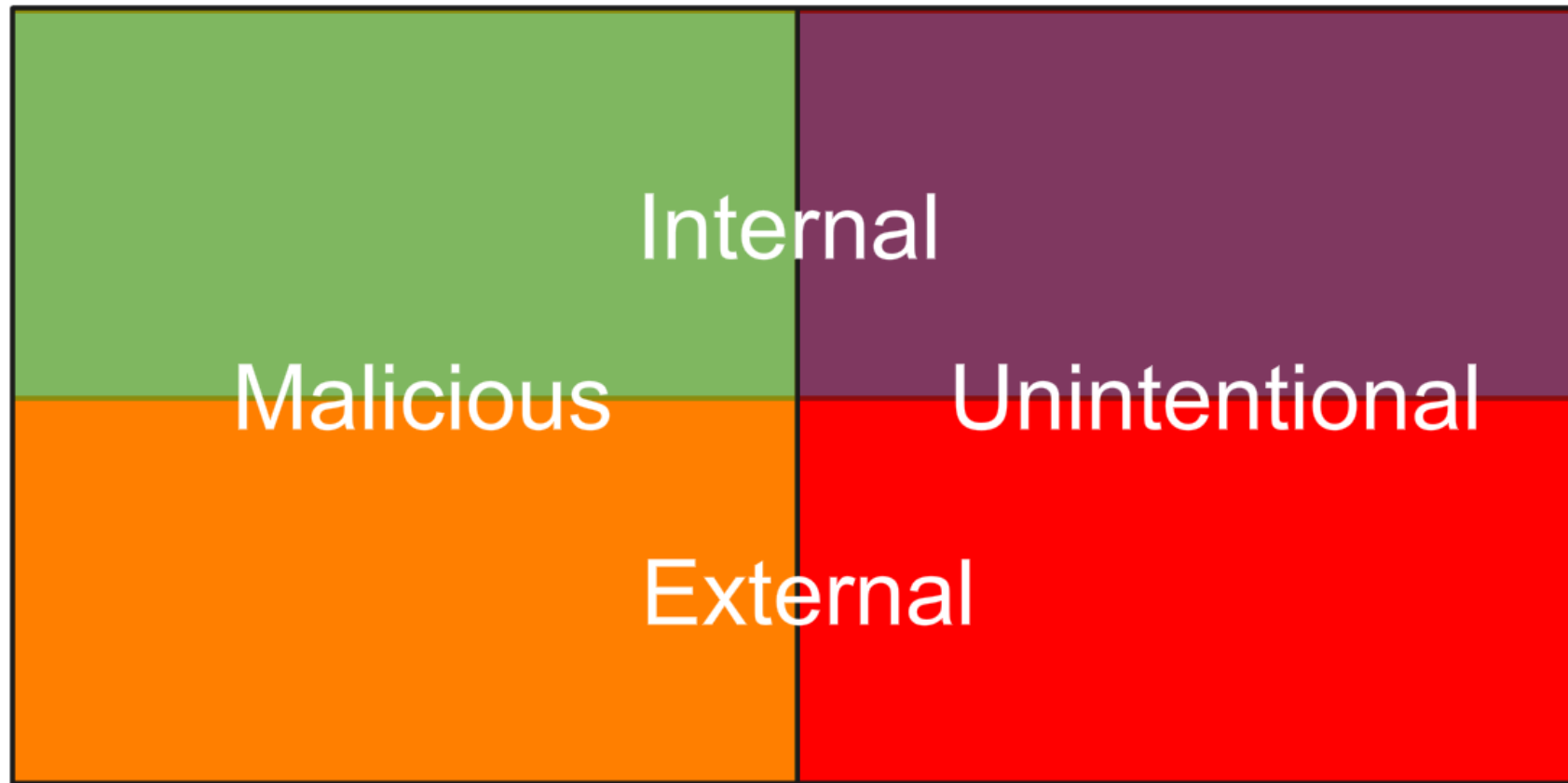
A decorative orange arrow pointing right, located in the top left corner of the slide.

Ways to help make security successful

- Limit the number of security decisions users need to make
 - Make it very simple for users to choose the right security action
 - Design to encourage consistent decision making whenever possible
 - Understand the school's needs
 - Empower a comprehensive view
- 
- A series of diagonal, light-colored lines running from the bottom left towards the top right, serving as a background design element.

From where do threats come?

The 4 Quadrants of Cyber Risk



HPN Risk Rate Process

We only use three categories

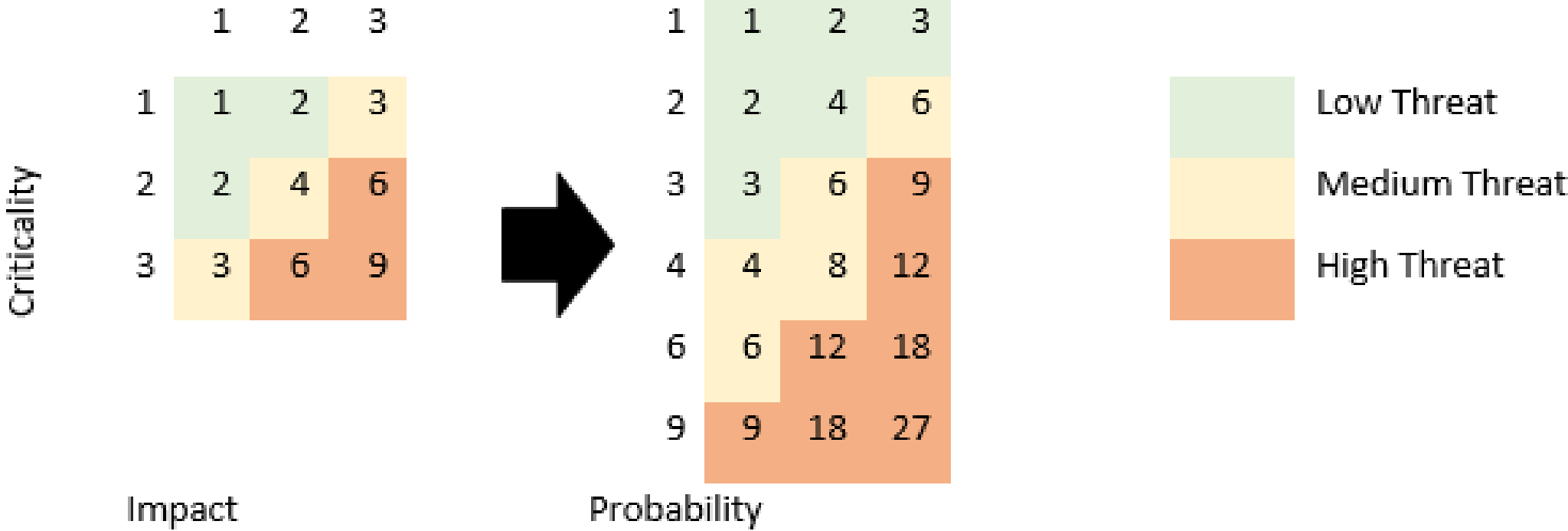
- If more than three categories are used, more time is spent trying to determine classification process
- Most people can classify into three categories without much thought
- Gives the granularity needed
- All three are measured 1-3 with 3 being the highest/worst

Criticality of the asset – 1=non-essential, 3= business critical

Impact of breach on confidentiality, integrity or availability – 1=low impact, 3= high impact

Probability of bad thing happening – 1=rare/low/miraculous, 3=eminent/high/common (think of viruses as high probability)

HPN Risk Rate Rankings



A decorative orange arrow pointing to the right, located in the top left corner of the slide.

Questions that need to be answered

- Do I know what is connected to our systems and network?
- Do we know what software is running (or trying to run)?
- Are we continuously looking for and managing “known bad” software?
- Do we limit and track people who have administrative privileges?
- Are we continuously managing our systems using “known good” configurations?


A decorative orange arrow pointing right, located in the top left corner of the slide.

What's connected to our network

- Active Discovery Tool
 - Active Ping Sweep
- Passive Discovery Tool
 - netFlow, jFlow, sFlow, IPFIX, port mirroring
- DHCP Logs
 - Can I tie back an IP address to a specific user and how far back can I go?

A decorative graphic on the left side of the slide, consisting of a vertical orange bar with a white arrow pointing right, and a blue vertical bar below it.

Shadow IT

- What is Shadow IT?
 - What are the drawbacks of Shadow IT?
 - Signs that Shadow IT is a problem
 - How to get ahead of Shadow IT
- 
- A series of diagonal, light pink lines that create a sense of movement and depth, extending from the bottom right towards the top left of the slide.

A large orange arrow graphic pointing to the right, partially overlapping the top left corner of the page.

Casino Gets Hacked

Internet-connected technology, also known as the Internet of Things (IoT), is now part of daily life, with smart assistants like Siri and Alexa to cars, watches, toasters, fridges, thermostats, lights, and the list goes on and on.

But of much greater concern, enterprises are unable to secure each and every device on their network, giving cybercriminals hold on their network hostage with just one insecure device.

Since IoT is a double-edged sword, it not only poses huge risks to enterprises worldwide but also has the potential to severely disrupt other organisations, or [the Internet itself](#).

SPONSORED SEARCHES

A set of four rounded rectangular buttons arranged in a 2x2 grid. The top-left button contains the text "Cyber Security Is", the top-right button contains "IoT", the bottom-left button contains "IoT and Cloud", and the bottom-right button contains "What Is IoT". A small blue play button icon is located to the right of the top-right button.

There's no better example than [Mirai](#), the botnet malware that knocked the world's biggest and [most popular websites offline](#) for few hours over a year ago.

We have another great example that showcases how one innocent looking [insecure IoT device](#) connected to your network can cause security nightmares.

Nicole Eagan, the CEO of cybersecurity company Darktrace, [told](#) attendees at an event in London on Thursday how cybercriminals hacked an unnamed casino through its Internet-connected thermometer in an aquarium in the lobby of the casino.

According to what Eagan claimed, the hackers exploited a vulnerability in the thermostat to get a foothold in the network. Once there, they managed to access the high-roller database of gamblers and "then pulled it back across the network, out the thermostat, and up to the cloud."

Although Eagan did not disclose the identity of the casino, the incident she was sharing could be of last year, when Darktrace published a report [\[PDF\]](#), referencing to a thermometer hack of this sort on an unnamed casino based in North America.

A decorative orange arrow pointing right, located in the top left corner of the slide.

What to do with the information

- Maintain an accurate and up-to-date inventory of all technology
 - How are IT purchases made?
- Use that information to address unauthorized assets
 - What is your process of being notified that an unauthorized asset is present?
 - How are unauthorized assets dealt with?
 - Who is responsible for dealing with unauthorized assets?

A decorative orange arrow pointing right, located in the top left corner of the slide.

Categorize Assets based on risk

- Any device that stores or accesses Personally Identifiable Information (PII)
- Servers/applications that can be accessed from the Internet
- Servers/applications that are used to ensure the operation of the school
- Administrative building user devices
- Teacher/staff devices
- Peripheral devices (printers, etc.)
- Student devices
- Environmental control devices (HVAC, etc.)

A decorative graphic consisting of two overlapping orange arrows pointing to the right, positioned at the top left of the slide.

Managing Software

- Maintain a list of approved software
 - All software should be vendor supported
- Utilize software inventory tools
- Use that information to address unauthorized software
 - What is your process of being notified that unauthorized software is present?
 - How is unauthorized software dealt with?
 - Who is responsible for dealing with unauthorized software?

A decorative graphic consisting of two overlapping orange arrows pointing to the right, located in the top-left corner of the slide.

Segmenting the network

Physically or Logically Segregate High Risk Applications or Devices

Physically or Logically Segregate Controlled and Uncontrolled Devices

Examples

- Any device(s) with PII
- Any device(s) that can access PII
- Any uncontrolled devices
- Applications that only run on non-supported operating systems
- Applications that require local administrative rights to run
- Demo software
- Environmental control software

Patch Management

	Q1 Top CVE	Q1 top Trigger	Q2 Top CVE	Q2 top Trigger	Q3 Top CVE	Q3 top Trigger
1	<u>CVE-2014-6332</u>	774	<u>CVE-2016-0189</u>	472	<u>CVE-2016-0189</u>	225
2	<u>CVE-2016-0189</u>	219	<u>CVE-2018-8174</u>	291	<u>CVE-2018-8174</u>	139
3	<u>CVE-2015-5122</u>	85	<u>CVE-2014-6332</u>	67	<u>CVE-2014-6332</u>	50

Table 1. Most triggered CVE Q1 to Q3 2018

A decorative orange arrow pointing right, located in the top left corner of the slide.

Patch Management

Deploy automated software update tools in order to ensure that Operating System software on all systems is running the most recent security updates

Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates

Don't forget about your infrastructure devices as well (firewalls, switches, wireless, printers, etc.)

A decorative graphic consisting of several overlapping orange arrows pointing to the right, located in the top-left corner of the slide.

Administrative accounts

- Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.
- Change all default passwords
 - Including SNMP strings
- Use dedicated accounts for administrative access
- Remove Local Administrator rights from users
- Use unique passwords
- Look to implement passphrases (15+ characters)
- Use multi-factor authentication where possible

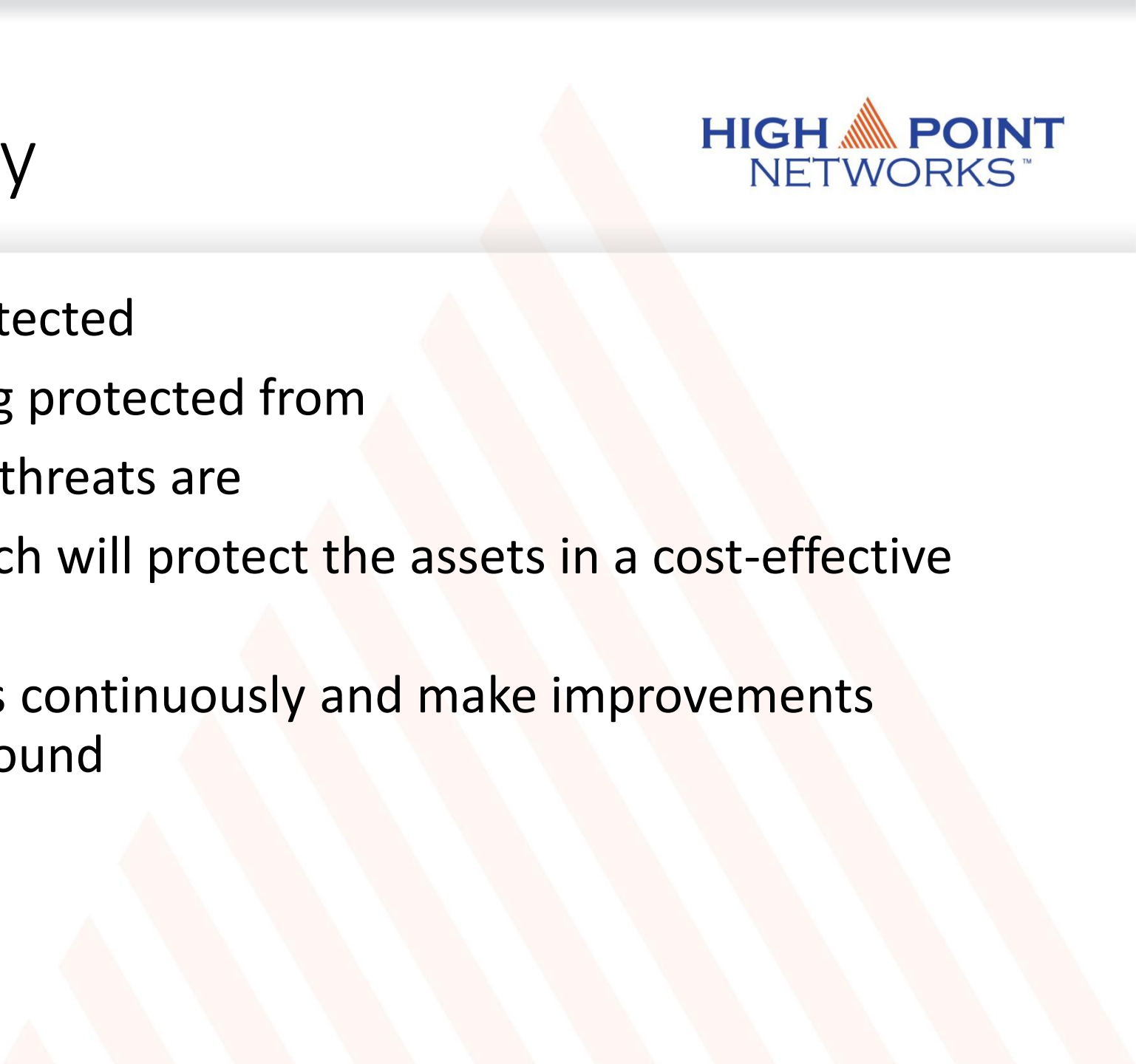
A decorative orange arrow pointing right, located in the top left corner of the slide.

Secure Configurations

- Maintain documented, standard security configuration standards for all authorized operating systems and software
- Create a change management process to help guide when images need to be updated
- Securely store the master images
- Deploy tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

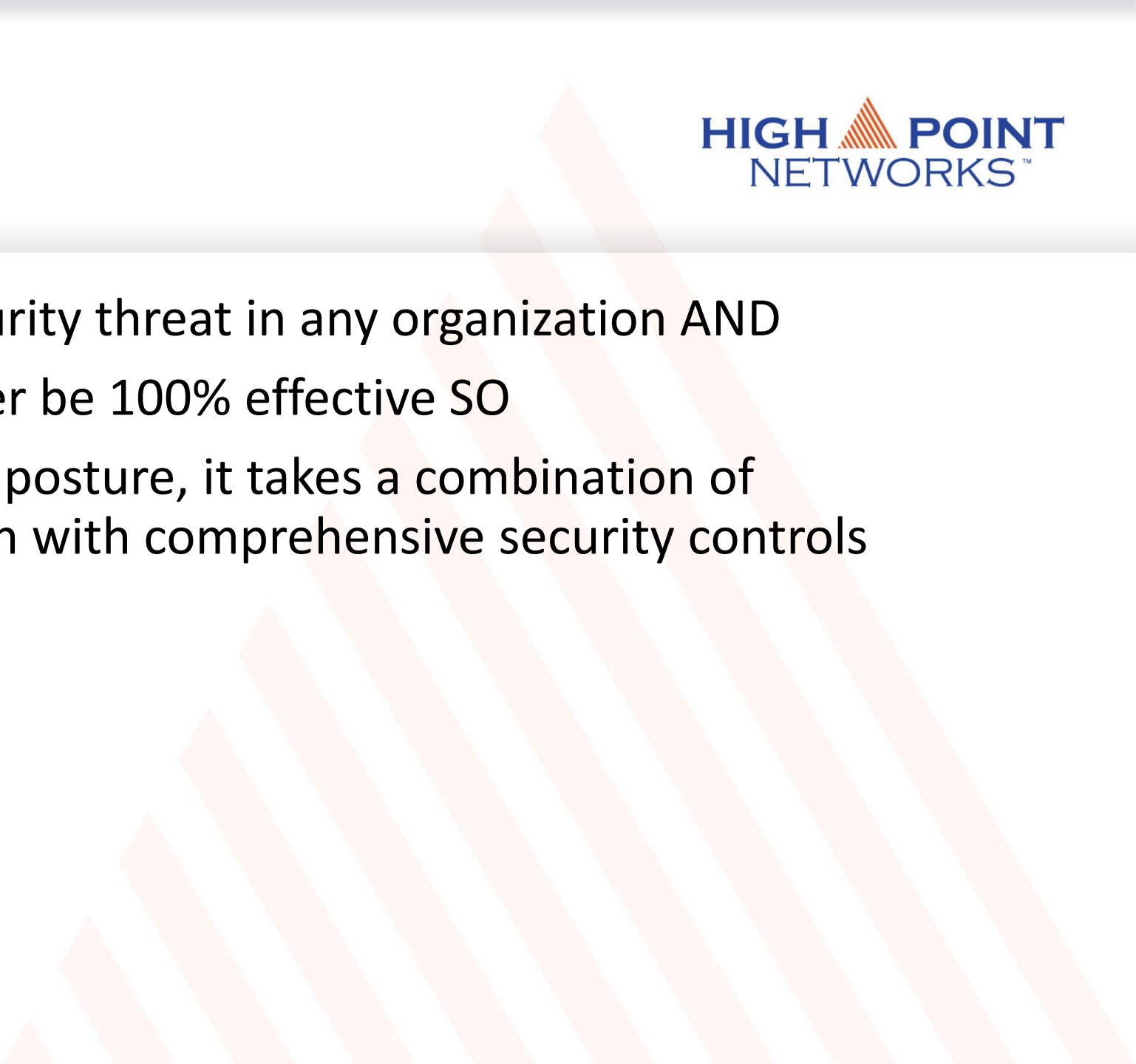
A decorative orange arrow pointing right, located in the top left corner of the slide.

Site Security Policy

- Identify what is being protected
 - Determine what it is being protected from
 - Determine how likely the threats are
 - Implement measures which will protect the assets in a cost-effective manner
 - Review the policy/process continuously and make improvements each time a weakness is found
- 
- A series of diagonal, light-colored lines extending from the bottom right towards the top left, serving as a background design element.

A decorative orange arrow pointing right, located in the top left corner of the slide.

Conclusion

- Users are the biggest security threat in any organization AND
 - Security controls will never be 100% effective SO
 - To improve one's security posture, it takes a combination of continuous user education with comprehensive security controls
- 
- A series of diagonal, light-colored lines running from the bottom left towards the top right, serving as a decorative background element.