NAME ABDULLAH KHAN ID 15270 QUESTION NO1

What is the difference between hazard and threat? Provide examples;

The takeaway here is that a **hazard** occurs (is "actualized") when your operations interact with **hazard** sources. A **threat** is simply a generic way to describe danger, whether the danger has actualized or not.

A **hazard is** something that can cause harm, e.g. electricity, chemicals, working up a ladder, noise, a keyboard, a bully at work, stress, etc

The six main categories of hazards are:

- Biological. **Biological hazards** include viruses, bacteria, insects, animals, etc., that can cause adverse health impacts. ...
- Chemical. Chemical hazards are hazardous substances that can cause harm. ...
- Physical. ...
- Safety. ...
- Ergonomic. ...
- Psychosocial.

A personal safety/security threat is defined as a situation which may be in the form of harassment, an assault, sexual assault, assault causing bodily harm, threat of assault, uttering threats of death/damage, of an individual, or any other act that constitutes a violent act as defined in the Criminal Code of Canada.

What Is a Specific Threat

A threat can also be a generic term for a specific danger, such as an object, situation, behavior, etc. A specific danger can be identified as:

- Contributing to rising danger – such as a hazardous source or contributing factor; or
- Representing actualized danger – such as a hazard occurrence.

Some examples are:

- "In spring time, migrating birds are a threat we have to mitigate";
- "That moose is no threat because he cannot get over the perimeter fence"; or
- "We have no plan for a bomb threat in our ERP."

A hazard in safety management is a condition that poses danger to your organization, and can lead to an accident, incident, or other mishap if not mitigates.

A hazard satisfies ALL of the following conditions:

- **Is a dangerous condition,** such as an object, situation, circumstance, that **poses an unacceptable level of danger**;
- **Occurs once** in the safety mishap lifecycle;
- **Can lead directly to risk occurrence** (i.e., safety mishap, accident, etc.) if not mitigated; and
- **Arise from hazard mechanisms**, such as initiating actions and hazardous sources.

Examples of Threats and Hazards EXAMPLES OF THREATS HAZARDS &			
Natural Hazards	**Technological Hazards**	**Biological Hazards**	**Adversarial, Incidental & Human** **Caused threat.**
• Earthquake • Tornado • Lightning • Severe Wind • Hurricane • Flood • Wildfire • Extreme Temperature • Landslide or Mudslide • Tsunami • Dust Storm • Volcanic Eruption • Winter Precipitation • Snow Storm • Other	• Hazardous materials in the community: industrial plants, tanker trucks on major highways or railroads • Radiological releases from nuclear power stations • Hazardous materials in the school: gas leaks, sewage break or laboratory spills • Infrastructure failure: dam, power, water systems, cyber • Other	• Infectious Diseases • Contaminated food outbreak • Water contamination • Toxic materials emerging in schools such as mold or asbestos • Toxic materials present in school laboratories • Other	• Fire or Explosion • Medical Emergency • Active Shooter • Threat of Violence • Fights • Gang Violence • Bomb Threat or Device found • Child Abuse • Cyber Attack • Cyber Malfunction • Suicide • Dangerous Person • Missing Student or Kidnapping • School Bus Emergencies • Student Demonstration or Riot • Dangerous Animal • Other

QUESTION NO 2: DEFINE RISK AND PROVIDE A CLASSIFICATION OF RISK BASED ON ITS SOURCES.PROVIDE AN EXAMPLE OF EACH RISK SOURCE.

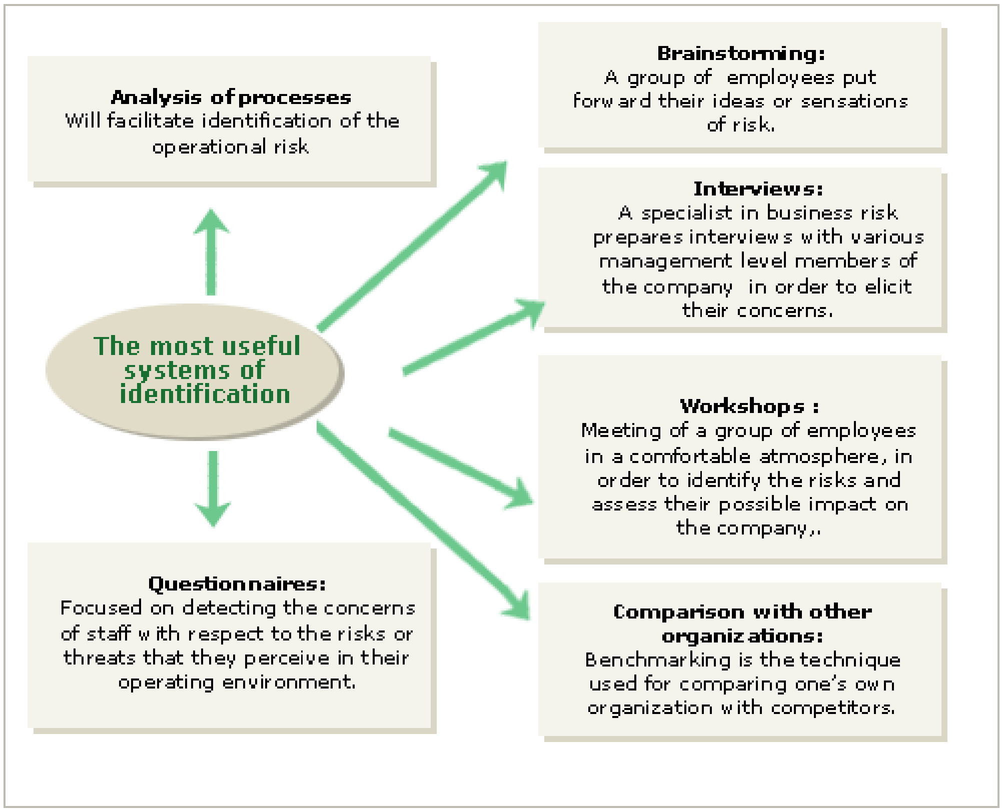
Risk

Description

Description

In simple terms, risk is the possibility of something bad happening. Risk involves uncertainty about the effects/implications of an activity with respect to something that humans value, often focusing on negative, undesirable consequences. Many different definitions have been proposed. Wikipedia

3.Other procedures for identifying risks:



The most useful systems of identification

Analysis of processes
Will facilitate identification of the operational risk

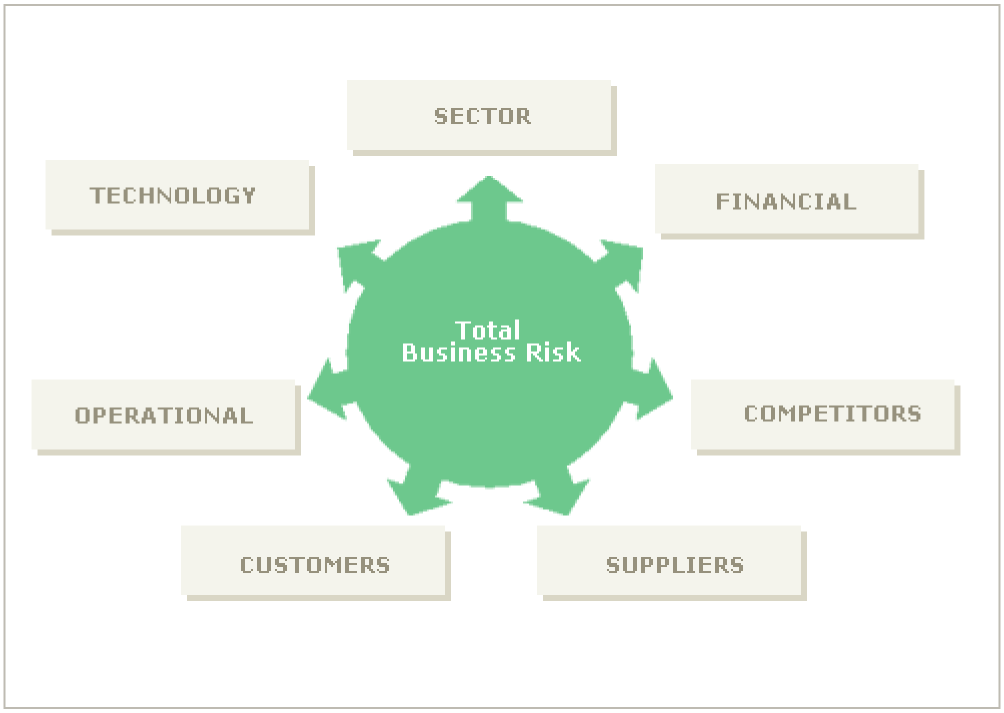
Questionnaires:
Focused on detecting the concerns of staff with respect to the risks or threats that they perceive in their operating environment.

Brainstorming:
A group of employees put forward their ideas or sensations of risk.

Interviews:
A specialist in business risk prepares interviews with various management level members of the company in order to elicit their concerns.

Workshops :
Meeting of a group of employees in a comfortable atmosphere, in order to identify the risks and assess their possible impact on the company,.

Comparison with other organizations:
Benchmarking is the technique used for comparing one's own organization with competitors.



4.Classification of risks:

□The purpose of the classification of risks is to show the risks identified in a structured manner, for example, in relation to their origin, as set out in the following graph.

SECTOR:

A risk that external factors independent from the entrepreneur’s management could directly or indirectly influence the achievement of his or her objectives and strategies to a significant extent.

Examples:

Strong exposure to regulatory changes
Business fragmentation
Appearance of new markets

OPERATIONAL:

The operational risks are associated with the entrepreneur’s ability to convert the strategy chosen into specific plans, by means of an effective allocation of resources.

Examples:

Need for making an advertising effort
High staffing costs
Lack of operational and financial planning
Tendency toward subcontracting. Tendency towards concentration

TECHNOLOGY:

This measures the entrepreneur’s exposure to the technological risks derived from the need to undertake heavy investment in order to ensure the feasibility of his or her business project within a specific period of time or the need for training the company’s employees in the use of the technology.

Examples:
Significant investments
Low level of implementation
Low level of technological training
COMPETITORS:
The size, the financial and operational capacity of the agents in a sector determine the degree of rivalry in that sector and set the rules of the game that any new agent has to consider in order to operate in the marketplace; this can involve risks for the entrepreneur.
Examples:
Appearance of new competitors
Intense competition
Specialized competition
SUPPLIERS:
The role played by the suppliers in the sector could generate risks for an entrepreneur due to variations in the price of raw materials, to the availability of a variety in the supply and for a continuous period of time, as well as the degree of concentration of the suppliers, which will determine the method of payment traditionally accepted in the sector.
Examples:
Exposure to changes in the price of goods
Dispersion in the supply
Non-determination of the quality of the service provided
Increase in power of negotiation

CUSTOMERS:
The customer can be a crucial focal point of risk for an entrepreneur, since they are the generators of revenues; the risk can stem from changes in their tastes and needs, from generating pressures forcing prices down or from lengthening the payment period, among other factors, in such a way that the entrepreneur's value proposal must always be customer-oriented.
Examples:
Increase in power of negotiation
Lack of loyalty
Social and demographic changes
Seasonality and decline in the demand
FINANCIAL:
The financial risks refer to the uncertainty associated with effective management and the control of finances carried out by the entrepreneur, as well as to the effects of external factors such as the availability of credit, exchange rates, movements in interest rates, etc.
Examples:
Long-term financial incapacity
Exposure to interest rate changes
Lack of knowledge of advantageous sources of financing, subsidies, etc

QUESTION NO 3:

HOW WOULD YOU ASSESS THE PERFORMANCE OF TRANSPORTATION SYSTEM OF A CITY.

ANSWER:

Why is transportation important in cities?
Reduced traffic congestion:
Public **transportation** can convey many more people in much less space than individual automobiles, which helps to keep traffic congestion lower, which in turn reduces air pollution from idling vehicles, and helps riders avoid the stress that comes from daily driving in highly congested areas.
What is the importance of transportation?
Transport is **important** because it enables communication, trade and other forms of exchange between people, that in turn establishes civilizations. **Transport** plays an **important** part in economic growth and globalization, but most types cause air pollution and use large amounts of land.Nov 20, 2013

Transport essential for growth in cities

Good transport connections have direct benefits to people, businesses, the environment, and the overall economy. For example, good transport can:

Help people access jobs. Good transport links can widen people's job-search area and help them find employment. It can also reduce commuting times and reduce the cost of living. Public transport is especially important for lower income groups, where 42 per cent lack access to a car or van (compared to only 8 per cent of those in the highest income group).[6] And high-skilled workers are more likely to travel across longer distances to work, especially if they are following Good transport connections have direct benefits to people, businesses, the environment, and the overall economy. For example, good transport can:

Help people access jobs. Good transport links can widen people’s job-search area and help them find employment. It can also reduce commuting times and reduce the cost of living. Public transport is especially important for lower income groups, where 42 per cent lack access to a car or van (compared to only 8 per cent of those in the highest income group).[6] And high-skilled workers are more likely to travel across longer distances to work, especially if they are following

Good transport connections have direct benefits to people, businesses, the environment, and the overall economy. For example, good transport can:

Help people access jobs. Good transport links can widen people’s job-search area and help them find employment. It can also reduce commuting times and reduce the cost of living. Public transport is especially important for lower income groups, where 42 per cent lack access to a car or van (compared to only 8 per cent of those in the highest income group).[6] And high-skilled workers are more likely to travel across longer distances to work, especially if they are following good job opportunities.

Support innovation, productivity and economic growth in cities and the national economy. Transport can encourage firms to locate near one another, bring them closer to their supply chain and share expertise. The increase in concentration (mainly referred to as ‘agglomeration economies’) improves firms’ performance and increases productivity.[8] A recent study in America found that doubling transport investment in cities raised productivity and increased wa**Help shape greener and healthier places.** Reducing the reliance on cars and promoting greener modes of transport (such as public transport or cycling) can relieve congestion and reduce carbon emissions. For example, London's road emissions per person are the same as Brighton's because of the efficient public transport network.[10] Good transport can also improve individuals' health and reduce healthcare costs. For example, if one in 10 journeys were made by bicycle, NHS could save £250 million per year.[11] ONS also found that personal wellbeing of commuters is reduced as the time needed to commute to work rises.[12]

Help cities attract new firms. Good transport networks can reduce costs and improve access to skilled labour. Reducing business and freight road travel time by 5 per cent can save business up to £2.5 billion every year (0.2 per cent of GDP).[13] Almost 60 per cent of UK firms consider transport infrastructure as a major influence on their business location.[14] And a U.S study found that the quality of airport facilities is the most important factor determining where global firms want to set up their headquarters.[15]

Unlock new development sites for business and housing. In order for new houses or businesses to be built, roads, bus services and rail must be in place to service them. The expansion and investment in Birmingham's New Street station is expected to drive a wider regeneration on the south side of the city as a part of the Big City Plan.[16] The Cambridge City Deal focused on much-needed transport investment to help the city keep up with the needs of growing businesses.[17]

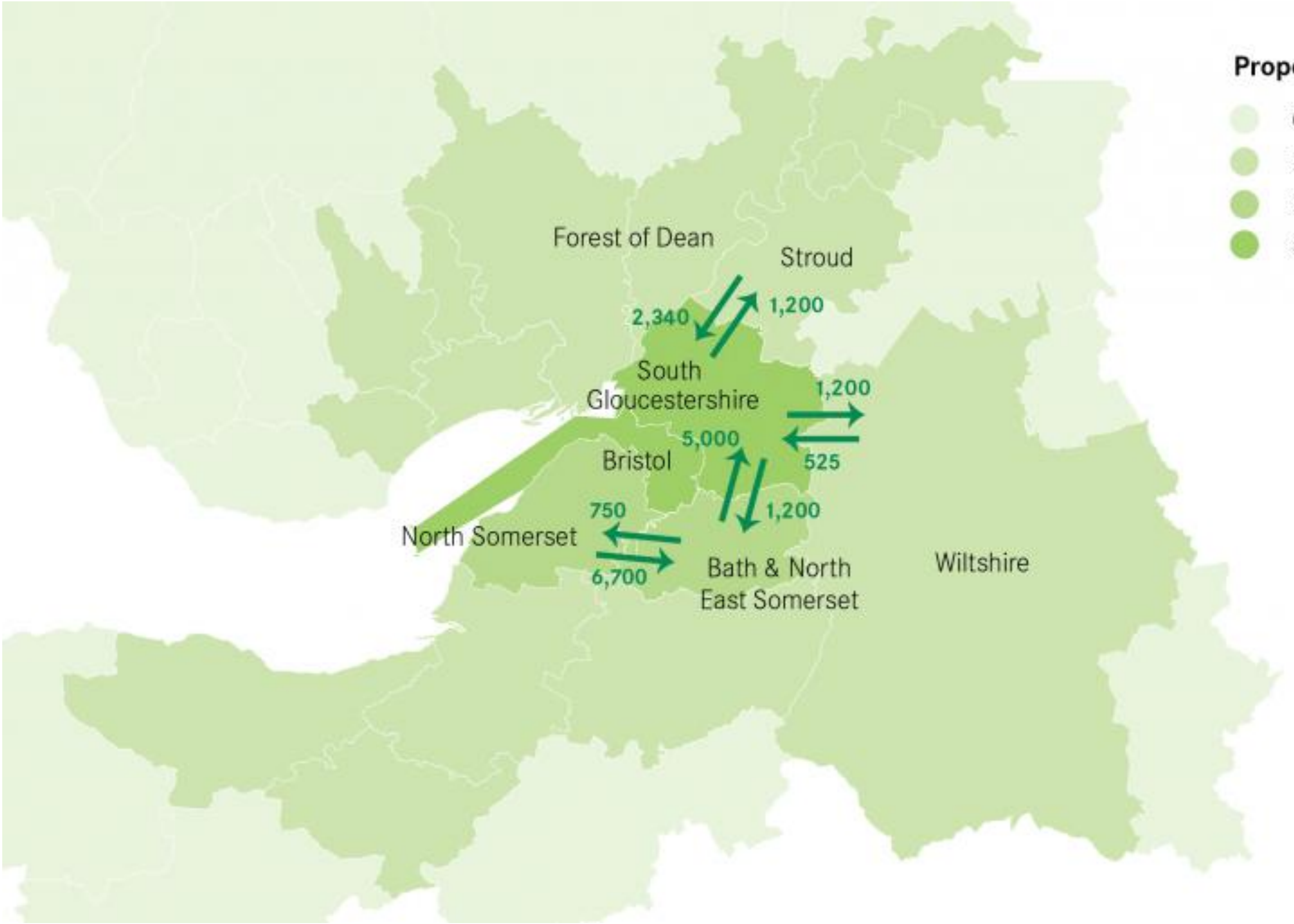
How do people use transport in cities?

In the UK almost half of commuters in cities live and work in different local authorities.[18] This means that transport systems — road, buses, trams, rail and cycling routes — must link various combinations of routes across the city region.

Transport crosses boundaries. The maps below demonstrate that while most of the people across a city region commute into the city centre for work, a large number of workers also commute between other local authorities. For example, more than 230,000 people commute to Manchester from across the UK. These come mainly from neighbours like Oldham and Tameside, but can also come from cities further afield such as Blackpool and York. At the same time, thousands commute between the areas surrounding Manchester every day. Around 90 per cent of journeys to a job in Greater Manchester start from a home in Greater Manchester.[19]

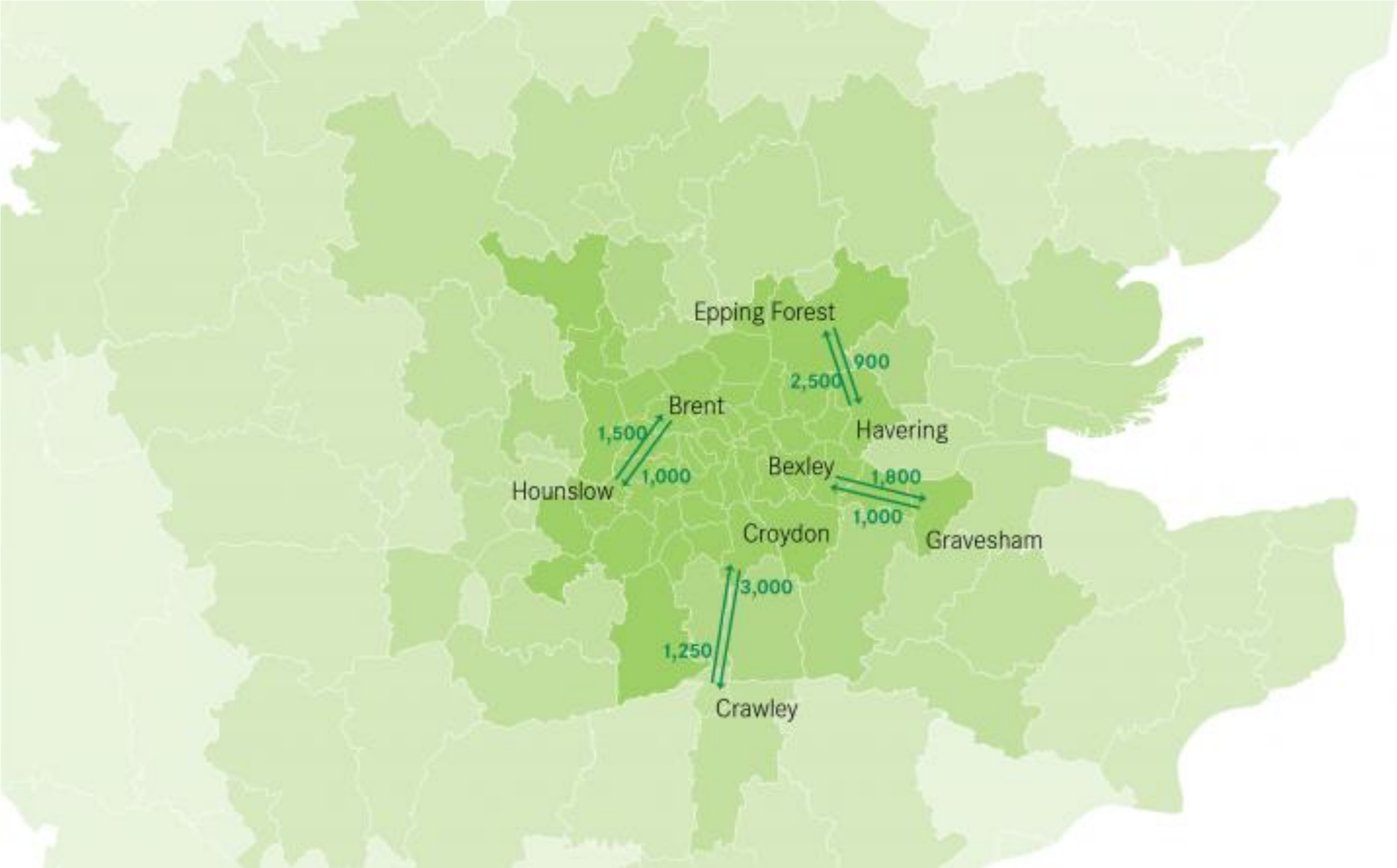
Figure 1: Commuting patterns in UK cities

Bristol



Propo
Forest of Dean
Stroud
2,340
1,200
South Gloucestershire
1,200
5,000
525
Bristol
750
1,200
North Somerset
6,700
Bath & North East Somerset
Wiltshire

London



QUESTION NO 4

ANSWER;

SECURITY VULNERABILITIES OF A UNIVERSITY CAMPUS:

Top 6 Higher Education Security Risks and Issues

Sometimes it seems like the security challenges facing American colleges and universities are never-ending.

Students and others share user information. Campus visitors pop USB sticks into networked machines. Hackers find their way into an internal network through carelessly discarded information from an open screen or from an infected workstation.

Here are six of the things that keep campus security people up at night, and big challenges that schools should address to make themselves more resistant to cyber threats.

Phishing and Social Engineering Attacks

One of the biggest challenges with university cybersecurity is the sheer amount of hacking that goes on in these environments. Schools have to deal with a unique mix of user levels, including students who are often young, and relatively trusting, and are not employees of the organization — so they're less controlled.

For example, research shows a full 90% of malware attacks originate through e-mail. Various types of spoofing and spear-phishing campaigns entice students and others to click on illegitimate links that can usher in a Trojan Horse to do damage to a network system, or compromise the security of information. Many of these kinds of phishing are cost, high — which leads to an inundation of hacker activity that schools have to keep in top of, by somehow segmenting network systems, by shutting down compromise parts of the system, or by some other high-tech means.

With this in mind, better security often starts with identifying separate pools of users — for example, administrative staff versus faculty and students, and then customizing controls and access for each of these groups individually.

The IT Crunch: Limited Resources

The challenge of limited resources and funding for university cybersecurity generally speaks for itself. The above kinds of network monitoring and cybersecurity engineering have significant costs attached to them, and many universities simply find it difficult allocate the manpower or the funding to address cybersecurity issues.

Regulatory Burdens and Secure Data Efforts

Another part of this challenging cybersecurity environment is that schools and universities have big compliance burdens under many different types of applicable regulation.

Some campus leaders tend to focus on items like NIST 800-171 and the use of controlled unclassified information, just because there is a deadline on for this particular type of compliance right now. However, regulations like

FERPA are also critical. Even HIPAA puts pressure on schools to tighten up cybersecurity, since as healthcare providers, schools may hold student health data. Third-party cloud providers often offer FEDRAMP certification and other qualifications for cybersecurity on their side of the fence — but that doesn’t fully bring a university into compliance unless it can bring its own internal systems up to standards.

System Malware — Zero Day Vulnerabilities and More

Universities and colleges also have to anticipate situations where hackers may exploit existing system vulnerabilities. They have to look at continuing support for operating systems and other technologies.

There is a reasonable expectation that manufacturers will make adequate security available, but this doesn’t absolve the university of having to look for security loopholes and close them. This means evaluating architectures — for example, can hackers get host names, IP addresses and other information from devices like printers?

It also means using multi-factor authentication to control user activity. It means understanding how malware will enter a system, and anticipating attacks. The good news is that modern security tools go well beyond the perimeter of a network to seek out harmful activity if they are set up right and controlled and observed well, they can dramatically decrease risk.

Protecting Personally Identifiable Information

At the heart of many of these cybersecurity efforts is the daunting struggle to protect all sorts of personally identifiable information, from simple student identifiers to financial data and medical data, from grades to Social Security numbers and items that identity thieves might use. The above-mentioned regulations are part of the drive to secure this type of data, along with more general standards and best practices for enterprise. Simply put, data breaches cost money, both in damage control, and in the reputation of the school itself.

In some ways, this ongoing data vigilance is hard for schools, because the academic world isn’t necessarily into strict control of information. But it’s also hard in a practical sense, because so many cybersecurity architectures just can’t handle modern challenges, like a WannaCry infiltration or other attacks that exploit common vulnerabilities. Many schools have up to a dozen or more security tools in place, but many of these tools don’t talk to each other or share data well, and so they become less effective as a comprehensive protective force.

There are some things that schools can do to protect PII — one technique is to limit end-user storage and access — for instance, restricting the ability of students to simply move floods of information to the cloud, or navigate sensitive internal network areas freely.

Another strategy is to use internal monitoring tools to inspect network traffic for suspicious activity.

For example, peeking at the header and footer of data packets can show the origin of data transfers, unless there is spoofing or some sophisticated type of deception involved. Some schools will go further and fully decrypt data packets to see what’s inside them. However, this practice can involve getting into the philosophy of privacy, where schools are wary of digging into network traffic because they see their monitoring as too intrusive to students or other users. In addition, emerging European privacy standards may put some pressure on schools in the U.S. to limit decryption and observation activities.

End-User Awareness and Training

Another way for schools to increase safety is for them to conduct vibrant types of end-user awareness campaigns.

This starts with educating end-users on how malware gets into a system — asking them not to click on suspicious e-mails or use inbound links, but instead to always do online banking and perform other transactions through a secure website.

Schools can also educate on the kinds of data that are most likely the targets of hacking activity — research data, student grades, health information or other sensitive data sets that hackers really want to get their hands on.

On the other side of the equation, schools should also work on improving their internal security postures — figuring out how they will respond to attacks, and how they will preemptively safeguard systems against everything from phishing to ransomware.