AlertFind

PANDEMICS, CYBER THREATS AND TERRORISM:

Don't Let These Emerging Threats Catch You Unprepared

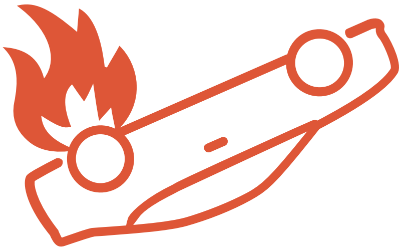
From the Sept. 11 attacks on the World Trade Center to the WannaCry ransomware attack, today's business risks are constantly evolving. Terrorism, cyber attacks and pandemics are the top emerging risks and organizations need to evolve their risk assessments to plan for them.

Previously, business continuity management used to be about safeguarding data and IT, but things have changed. Our knowledge of which business assets we need to protect and what we what we need to do to protect them has matured.

Terrorism's Growing Impact

The threat from terrorism, in fact, can be traced back centuries, but it continues to evolve and proliferate. The term dates back to the French Revolution and the Reign of Terror.

Between June 1793 and July 1794, close to 17,000 people were sent to the guillotine by the fledgling French Republic. Fast-forward to today, and between 1970 and 2017, about 181,000 global terrorist attacks were recorded. Of these, 50% used explosives and about a third used firearms.



Terrorists have three goals when perpetrating an attack:

- Maximize the damage to critical assets
- Maximize human casualties
- Popularize their cause with media coverage of the attacks

In addition to shootings and bombings, terrorists are incorporating new weapons into their attacks.

Vehicle Attacks

In Nice, France, a vehicle was used as a battering ram and driven into a crowd of people attending a Bastille Day event in 2016. The incident left about 85 dead and 300 badly injured.

Terrorists now routinely use this tactic all over the world. In 2017, a car drove into a crowd of pedestrians at Times Square in New York, killing one and injuring at least 22 people. This type of act does not need a large, expensive, coordinated support system. It can be carried out by a lone wolf terrorist, which is difficult to detect or plan for.

There has also been a rise in vehicle-ramming incidents. Between 1917 and 2013, there have been 69 incidents. In the last four years, however, there have been more than 80 such incidents — 13 in the U.S., 12 in the U.K., and about 62 incidents in the Middle East.

Drone Attacks

Another emerging threat is drones, particularly drone swarms, where many drones are used to target and disable commercial aircraft. Individual drones have caused near-misses in the air and some have even collided with aircraft.

In January, a Russian airbase in Syria was attacked by about a dozen drones rigged with explosives. The Russians managed to shoot down seven using anti-aircraft missiles, and electronically disabled the remainder.

Between 1917 and 2013, there have been 69 vehicle attacks. In the last four years, however, there have been more than 80 such incidents.

The 2002-2003 severe SARS outbreak spread to 26 countries before the World Health Organization was even aware of its existence.

Global Pandemics

Pandemics, infectious illnesses that spread globally and have no cure or vaccine, have been a threat much longer than terrorism. In the 20th century, three were recorded. Two were considered relatively mild with only three million fatalities recorded globally. The Spanish Flu pandemic in 1918, however, was considered severe, with more than 50 million deaths recorded globally. Pandemics do not differentiate between age, sex or social class. And as we have seen, their effects are devastating.

Global Air Travel Expected To Aid Pandemic Spread

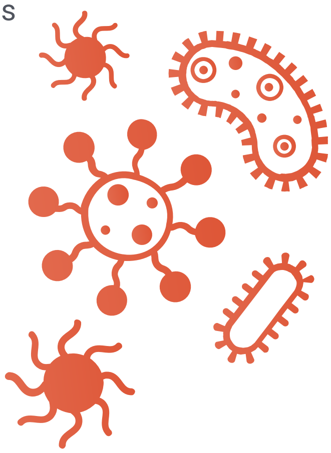
In September, a United Emirates aircraft from Dubai arrived at John F. Kennedy International Airport with around 100 of the more than 500 passengers and crew on board showing flu-like symptoms.

Eleven required hospitalization. This was an isolated incident, and it was quickly contained, but experts believe this is how a pandemic will spread — through global air travel.

We learned from the 2002-2003 severe SARS outbreak that modern-day aviation can facilitate dispersion of an illness around the world in a matter of hours. In fact, SARS spread to 26 countries before the World Health Organization was even aware of its existence. These incidents tell us that we must begin planning and preparing now for the business effects of the next pandemic.

Pandemics Are Top Global Risk

With the many threats businesses need to plan for, pandemics shouldn't be overlooked. In fact, virtually every national risk register now has one thing in common: pandemics are flagged as a major threat we are now facing.



This threat is a potential civil emergency that cannot be ignored, as it could impact businesses in many ways. Employees are vulnerable, but so are supply chains and your customer base. Organizations that are prepared can reduce risk as well as help protect their employees, suppliers and customers.

Cyber Attacks Are Booming

Cyber attacks are a persistent and growing threat that companies and governments ignore at their own peril. An astonishing 700,000 new threats are identified every day.

"If you believe this threat doesn't apply to you, I remind you of what former FBI Director Robert Mueller III said, 'There are two types of companies: those that have been hacked, and those that are going to be hacked,'" said Robert Clark, a business continuity expert in a recent AlertFind webinar, Pandemics, Terrorism and Cyber Attacks: Is Your Organization Ready for the Evolving Risk Landscape?

It doesn't matter whether your organization is a global corporation or a small to medium-sized enterprise - each one is at risk. Last year it was estimated that about 59% of all cyber attacks targeted small and medium-sized enterprises.

When the internet was first created, very little thought was given to security. And that omission has caused major problems ever since. In fact, the Business Continuity Institute (BCI) has identified cyber attacks as the top threat for the third year in a row. This risk should feature prominently in every company's risk assessment, no matter the size of the enterprise.

Three defining events heralded the age of cyber threats:

Fiction Predicts The Future

In 1983, “War Games,” a film about a juvenile delinquent who managed to hack into the NORAD (North American Aerospace Defense Command) computers and came very close to starting World War III, was released. The film raised the profile of cyber threat considerably.

In fact, after seeing the film, President Ronald Reagan asked his security team if such an event was possible. The answer was yes, which prompted the government to start preparing for this scenario.

About 14 years later, a 15-year-old did manage to penetrate U.S. Air Force computers on Guam. While not quite as destructive or dangerous as a NORAD intrusion, it made clear the continuing vulnerability of our vital national security network.

State-Sponsored Cyber Attacks

The second serious event occurred in 2007, when the Baltic state of Estonia, which is now part of NATO, was the target of a massive distributed denial-of-access attack. It effectively closed down the Estonian Parliament and all government ministries, as well as banks and the media.

```
> .sf-sub-indicator
ent .cart-menu .cart-icon-wr
der-outer.transparent header#top
nav .sf-menu > li.current_page
nav .sf-menu > li.current-menu-
nav > ul > li > a:hover > .sf-sub
nav ul #search-btn a:hover span,#
nav .sf-menu > li.current-menu-ite
hover .icon-salient-cart,.ascend
:!important;color:#ffffff!impo
parent header#top nav>ul>li.but
widget-area-toggle a i
```

An astonishing 700,000 new threats are identified every day.

It turned out that the attack was perpetrated by Russians, who were apparently upset that Estonia was relocating a bronze statue — an elaborate Soviet-era war grave monument erected by the Soviet Union. Observers believe that this state-sponsored cyber attack was one of the most sophisticated ever seen at that time.

Ransomware Attacks

WannaCry is a massive ransomware attack estimated to have infected a quarter-million computers across 150 countries in May 2017. Organizations it affected included household names such as FedEx in the U.S. and the U.K.'s National Health Service.

WannaCry was designed to spread quickly among computers on the same network, and then encrypt the victim's own files, when hackers would then demand ransom from users for the key to release the computer files.

Hackers Exploit IoT Devices

Hackers continue finding ways to penetrate seemingly secure computer networks. When they targeted a casino's high-roller database, they gained access through the thermometer in the lobby's fish tank, which was connected to the internet. This type of Internet of Things attack makes a growing number of devices vulnerable.

The message is clear: any computer network that is connected to the internet is vulnerable. And no one is immune to cyber attacks. Four years ago, there were about 300,000 new threats daily. Today, it's 700,000 new threats and experts expect it to keep growing exponentially.

Threats are everywhere, ranging from smartphones to servers and every device in between. Remember, anyone who is connected by any device to the internet is at risk, whether it's the fish tank in your lobby or the smartphone in your pocket.

It is recommended that a business impact analysis be done at least once a year.

Risk Assessments Must Include These Threats

The World Health Organization (WHO) states that business continuity plans "are at the heart of preparing all levels and groups of society for an emergency."

What's more, because the threats are always changing, risk assessment and planning also must evolve to keep organizations prepared for the latest risks.

It is recommended that a business impact analysis be done at least once a year unless there is a major change within the company such as an acquisition or merger, new product introductions or discontinued goods or services.

If an organization doesn't have a risk management function, then the responsibility most likely falls to the business continuity manager to perform a risk assessment. They need to be prepared by knowing what's going on both within the company and around the globe. Vigilance is vital.

An important factor across all of these threats is globalization. Consequently, seemingly unimportant events that occur on the other side of the planet can seriously impact your global supply chains and therefore need to be factored into your risk assessments.

Build Knowledge With These Resources

When working on your organization's risk assessment, local, state and federal agencies all offer information and resources to aid in your planning

Local and national governmental agencies offer detailed information and tracking tools covering all the major threats. There are also industry publications and news sites that track each of these risks.

Here are some resources to get you started:

Terrorism

- Global Terrorism Database
- DHS: Preventing Terrorism
- Vehicle Attacks
- NYPD Shield

Pandemics

- Business Continuity and the Pandemic Threat
- FEMA: Pandemic Influenza Template
- CDC: Pandemic Strategy
- WHO: Influenza Pandemic Preparedness
- TEDEd Talk on Pandemics

Cyber Threats

- Symantec 2018 Internet Security Threat Report
- Cyber Threat Real-Time Map
- DHS: Cybersecurity Strategy
- McAfee on New Cyber Threats

General Information

- Continuity Central
- Business Continuity Institute
- DRI International
- Disaster Recovery Journal
- SAFE: How to stay safe in a dangerous world

Now is the time to take action and update your organization's risk assessment to reflect these emerging risks. Your organization must have a plan in place to deal with these threats before they strike.

Ready to learn more about dealing with these emerging risks?

Watch the webinar with expert Bob Clark to see how you can better protect your organization.

Watch the Webinar

About the author

Robert Clark is a Fellow of the Institute of Business Continuity Management, a Fellow of the British Computer Society and a Member of the Security Institute. His career includes 15 years with IBM and 11 years with Fujitsu Services, working with clients on BCM-related assignments.

The author of a number of business continuity-related publications, Bob wrote “Business Continuity and the Pandemic Threat” as well as his newest book, “Crisis Management: Is Social Media Its New Best Friend Or Its Worst Nightmare?” He works with a number of global businesses through his company, BCM Consultancy.

Af | AlertFind