Incident Response

== History == be5aa1c7fe == History == be5aa1c7fe SiRT is headed by a civilian director, who has never been a police officer. The Director is responsible for the overall operations of the agency, and to review all investigative reports. The Director has the sole power to determine whether any charges will be laid against subject officers, unless the Director is on leave. During his absence, a specially-trained Crown Counsel is appointed as the Acting Director to decide whether charges are laid. be5aa1c7fe An incident response plan (IRP) is a group of policies that dictate an organizations reaction to a cyber attack. Once a security breach has been identified, for example by network intrusion... be5aa1c7fe In response to public outcry over the standoffs at Ruby Ridge, Idaho, and of the Branch Davidians in the Waco siege, the FBI formed the CIRG in 1994 to deal with crisis situations more efficiently. The CIRG is designated to formulate strategies, manage hostage or siege situations, and if possible resolve them "without loss of life", as pledged in a 1995 Senate hearing by FBI director Louis Freeh, who assumed the post four-and-a-half months after the Waco Siege. be5aa1c7fe

Computer security incident management incident management involves the monitoring and detection of security events on a computer or computer network, and the execution of proper responses In the fields of computer security and information technology, computer security incident management involves the monitoring and detection of security events on a computer or computer network, and the execution of proper responses to those events. Computer security incident management is a specialized form of incident management, the primary purpose of which is the development of a well understood and predictable response to damaging events and computer intrusions be5aa1c7fe

Incident response team Incident response teams are common in public service organizations as well as in other organizations, either military or specialty. An incident response team (IRT) or emergency response team (ERT) is a group of people who prepare for and respond to an emergency, such as a natural disaster An incident response team (IRT) or emergency response team (ERT) is a group of people who prepare for and respond to an emergency, such as a natural disaster or an interruption of business operations. This team is generally composed of specific members designated before an incident occurs, although under certain circumstances the team may be an ad hoc group of willing volunteers be5aa1c7fe

Incident Commander – oversees all operations at the incident. be5aa1c7fe FIRST was founded as an informal group by a number of incident response teams after the WANK (computer worm) highlighted the need for better coordination of incident response activities between organizations, during major incidents. It was formally incorporated in California on August 7, 1995, and moved to North Carolina on May 14, 2014. be5aa1c7fe An incident is an event that may lead to the loss of, or disruption to, an organization's operations, services or functions. Incident management (IcM) is a term describing the activities of an organization to identify, analyze, and correct hazards to prevent a future re-occurrence. If not managed, an incident can escalate into an emergency, crisis or disaster. Incident management is therefore the process of limiting the potential disruption caused by such an event, followed by a return to business as usual. Without effective incident management... be5aa1c7fe == Organization == be5aa1c7fe Incident response team members ideally are trained and prepared to fulfill the roles required by the specific situation (for example, to serve as incident commander in the event of a large-scale public emergency). As the size of an incident grows, and as more resources are drawn into the event, the command of the situation may shift through several phases. In a small-scale event, usually only a volunteer or ad hoc team may respond. In events, both large and small, both specific member and ad hoc teams may work jointly in a unified command system. Individual team members can be trained in various aspects of the response, either be it medical assistance/first aid, hazardous material... be5aa1c7fe

Incident management These incidents within a structured organization are normally dealt with by either an incident response team (IRT), an incident management team An incident is an event that could lead to loss of, or disruption to, an organization's operations, services, or functions. recurrence. Without effective incident management, an incident can disrupt business operations, information security, IT systems, employees, customers, or other vital business functions. These incidents within a structured organization are normally dealt with by either an incident response team (IRT), an incident management team (IMT), or Incident Command System (ICS). Incident management (IcM) refers to the activities an organization undertakes to identify, analyze, and correct hazards to prevent future recurrence be5aa1c7fe

usually one of the first officers on... be5aa1c7fe

Forum of Incident Response and Security Teams The Forum of Incident Response and Security Teams (FIRST) is an American multinational organization with incident response team organizations for information The Forum of Incident Response and Security Teams (FIRST) is an American multinational organization with incident response team organizations for information security as its members be5aa1c7fe

Incident management requires a process and a response team which follows this process. In the United States, This definition of computer security incident management follows the standards and definitions

described in the National Incident Management System (NIMS). The incident coordinator manages the response to an emergency security incident. In a Natural Disaster or other event requiring response from Emergency services, the incident coordinator would act as a liaison to the emergency services incident manager. be5aa1c7fe CIRG was intended to integrate tactical and investigative resources and expertise for critical incidents which necessitate an immediate response from law enforcement authorities. CIRG will deploy investigative specialists to respond to terrorist activities, hostage takings, child abductions and other high-risk repetitive violent crimes. Other major incidents include prison riots, bombings, air and train crashes, and natural disasters... be5aa1c7fe Other names used to describe CERT include cyber emergency response team, computer emergency readiness team, computer security incident response team (CSIRT), or cyber security incident response team. be5aa1c7fe

FBI Critical Incident Response Group CIRG enables the FBI to rapidly respond to, and effectively manage, special crisis incidents in the United States. The Critical Incident Response Group (CIRG) is a division of the Criminal, Cyber, Response, and Services Branch of the United States Federal Bureau of The Critical Incident Response Group (CIRG) is a division of the Criminal, Cyber, Response, and Services Branch of the United States Federal Bureau of Investigation (FBI) be5aa1c7fe

The name "Computer Emergency Response Team" was first used in 1988 by the CERT Coordination Center (CERT-CC) at Carnegie Mellon University (CMU). The term CERT is registered as a trade and service mark by CMU in multiple countries worldwide. CMU encourages the use of Computer Security Incident Response Team (CSIRT) as a generic term for the handling of computer security incidents. CMU licenses the CERT mark to various organizations that are performing the activities of a CSIRT. be5aa1c7fe

Special Operations Engineer Regiment (Australia) 2002 as the Incident Response Regiment (IRR), they are deployed to respond to chemical, biological, radiological, nuclear or explosive incidents. The regiment The Special Operations Engineer Regiment (SOER) is a specialised unit of the Australian Army. In 2010 and 2011, its role changed to supporting the army's special forces units, and it was renamed accordingly. The regiment forms part of the Special Operations Command. The unit was formed in 2002 as the Incident Response Regiment (IRR), they are deployed to respond to chemical, biological, radiological, nuclear or explosive incidents. The regiment was transferred into the newly raised Special Operations Command in 2003 be5aa1c7fe

== History == be5aa1c7fe

Critical Incident Response Team CIRT was formed to conduct regular patrols of metropolitan Melbourne 24-hours, seven-day-per-week, ready to rapidly respond to incidents in Melbourne, and if necessary, in regional Victoria, by a small team of officers. CIRT has evolved to include conducting planned operations for high risk searches and arrests. The Critical Incident Response Team (CIRT) is a specialist unit of the Victoria Police that provides assistance to general duties police, including a The Critical Incident Response Team (CIRT) is a specialist unit of the Victoria Police that provides assistance to general duties police, including a negotiator capability, to resolve high risk incidents utilising specialist tactics and equipment be5aa1c7fe

In 1999, the Joint Incident Response Unit (JIRU) was established as part of the Australian Defence Force's security arrangements for the 2000 Sydney Olympic Games. The JIRU incorporated... be5aa1c7fe The Special Operations Engineer Regiment (SOER) can trace its history to a number of specialist Royal Australian Engineers organisations. The Emergency Response Squadron was initially formed in 1999 from the existing Army Fire Service in response to the 1996 Blackhawk Helicopter disaster in the Townsville High Range training area. The Chemical, Biological and Radiological Response (CBRR) Squadron was formed in 1999 by expanding the existing Chemical Radiological Response Team. be5aa1c7fe SiRT is one of the three investigative oversight agencies for police in Canada (the other being the Independent Investigation Unit of Manitoba and Alberta Serious Incident Response Team) to have current sworn police officers from the Province appointed as... be5aa1c7fe == Description == be5aa1c7fe The histories of CERT and CSIRT, are linked to the existence of malware, especially computer worms and viruses. Whenever a new technology arrives, its misuse is not long in following. The first worm in the IBM VNET was covered up. Shortly after, a worm hit the Internet on 3 November 1988, when the so-called Morris Worm paralysed a good percentage of it. This led to the formation of the first... be5aa1c7fe == Incident response plans == be5aa1c7fe

Serious Incident Response Team The Serious Incident Response Team is the civilian oversight agency in Nova Scotia, Canada responsible for the investigation of incidents resulted in The Serious Incident Response Team is the civilian oversight agency in Nova Scotia, Canada responsible for the investigation of incidents resulted in serious injury or death to any person, sexual assault and domestic violence allegations and other significant public interest matters concerning the police. SiRT has jurisdiction over all municipal police officers and Royal Canadian Mounted Police "H" Division officers, and for all complaints whether on- or off-duty related be5aa1c7fe

Computer emergency response team A computer emergency response team (CERT) is an incident response team dedicated to computer security incidents. Other names used to describe CERT include A computer emergency response team (CERT) is an incident response team dedicated to computer security incidents be5aa1c7fe

== History == be5aa1c7fe

Incident commander The incident commander may, at their own discretion, assign individuals, who may be from the same agency or from assisting agencies, to subordinate or specific positions for the duration of the emergency. The Incident Commander sets priorities and defines the organization of the incident response teams and the overall incident action plan. Even if subordinate positions are not assigned, the Incident Commander position will always be designated or assumed. The Incident Commander is the person responsible for all aspects of an emergency response; including quickly developing incident objectives, managing all The Incident Commander is the person responsible for all aspects of an emergency response; including quickly developing incident objectives, managing all incident operations, application of resources as well as responsibility for all persons involved. The role of Incident Commander may be assumed by senior or higher qualified officers upon their arrival or as the situation dictates be5aa1c7fe

== History == be5aa1c7fe == The incident command system in a Canadian EMS scenario == be5aa1c7fe In the United States, most agencies use an Incident Commander for the roles and responsibilities as defined under the National Incident Management System as a part of the Incident Command System. be5aa1c7fe