Case Studies

Sample Freezer Control Systems

Tissue and other samples and some reagents used for research are commonly stored in carefully controlled refrigerators and freezers. These are tightly controlled and monitored by temperature sensors to accurately maintain a specific temperature withing a very tight tolerance. Slight deviations in temperature can cause the loss of samples which may be challenging if not impossible to replace and might represent years of work and/or millions of dollars to collect.

Information Security Risk Classification: **Low Risk Information** – The temperature control systems are only processing numeric data that is not sensitive in any way. It could be (and sometimes is) displayed on public monitors without incident.

Electronic Service Risk Classification: **High Risk Service** – Compromise or failure of these control systems could result in the loss of millions of dollars, the inability to complete research projects, and/or failure to meet funder requirements for biobank retention. This could likely become a major media story that would significantly impact UBCs reputation.

Note: From an Information only perspective this would be considered a Low-Risk Service, but the Electronic Service Risk Classification is always informed by the factors that cause the greatest risk to UBC.

Name of Case Study: Electronic Door Locks

Key-card access control systems collectively grant/revoke building access permissions as well as allow entry to authorized individuals. In the event of loss of availability broad access to campus facilities may be disabled causing operational disruption. Student and employee names are captured in some of these systems. In most cases physical access can be granted by Campus Security staff, so it is difficult to envision prolonged operational difficulties impacting most of UBC. However, if the access systems were to fail in an open state this could result in security incidents in data centers or sensitive research labs with loss of significant personal information or intellectual property.

Information Security Risk Classification: **High-Risk Information** – Access Control Systems frequently store student names, but no further very-high risk information such as government IDs.

Electronic Service Risk Classification: **Very-High Risk Service** – Compromise or failure of key-card access control systems could result in security incidents with massive impact on UBC reputation.

Name of Case Study: Dental Clinic

A UBC Dental Clinic runs an Electronic Medical Records (EMR) system with around 20,000 patient records containing medical heath information. While the availability of the system is necessary for the day-to-day operations of the clinic, if unavailable for a period of time, it would not prevent all appointments, and emergency dental procedures could still proceed.

Information Security Risk Classification: **Very-High Risk Information** – The EMR contains significant volumes of personal health information of some degree on all patients. Personal Health Information is Very-High Risk information.

Electronic Service Risk Classification: **Very-High Risk Service** – Ignoring the electronic information contained within the service this would be a Medium Risk Service due the normal administrative operational impact of a loss of availability. However, due to the Very-High Risk Information, potential harm to individuals if compromised and the reputational and financial implications of an incident, this is Very-High Risk Service.

Name of Case Study: Central Accident and Incident Reporting System

UBC runs a service to capture and report health & safety incidents report health & safety incidents and near misses for the purposes of meeting WorkSafeBC regulations. A process exists to remove submitted personal health information which is not relevant to the incident, and the remaining information is unlikely to cause harm to individuals if made public.

Information Security Risk Classification: **High-Risk Information** – The system contains personal information of UBC constituents who have been the subject or a report/have submitted a report.

Electronic Service Risk Classification: **Medium-Risk Service** – Although administrative difficulties would be experienced if the service was unavailable, workarounds are possible mitigating impact. Although the service contains high-risk information (personal information in this case), it is unlikely there would be harm to the individuals if the information was made public, which in turn reduces likely costs and reputational risk to UBC.

Departmental Web Site

Many UBC departments publish a departmental web site with information about the activities of the department, news, and contact information. This information is entirely intended for public disclosure and is used exclusively for informational purposes. Cases where a web site also includes an area requiring authentication are not included in this example.

Information Security Risk Classification: **Low Risk Information** – The information is already public and intended for disclosure.

Electronic Service Risk Classification: **Low Risk Service –** Should the site need to be taken offline due to compromise or to mitigate a vulnerability the impact is minimal. Most of the information would likely be available through other means and even an outage of multiple days would not pose a significant impact to the institution.

Related Documents

U1, Security Classification of UBC Electronic Information and Services
Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems