	Ordinary (Impact is minimal)	Medium (Impact is moderate)	Severe (Impact is significant)
Attack			
Externally initiated Flood/Distributed Denial of Service	Considerable network resources are being consumed with minimal impact on network performance	A malicious user consumes network resources which impedes non-mission critical services for a noticeable duration	A malicious user consumes network resources which impedes: * internal mission critical services * network performance originating from multiple external hosts
Internally initiated Flood/Distributed Denial of Service	A legitimate application consumes a noticeable amount of network resources	A malicious user consumes network resources which impedes non-mission critical services for a noticeable duration	A malicious user consumes network resources which impedes: * internal mission critical services * sensitive machines external to the University
Sabotage/defacement	System sabotaged and a suitable backup may be available. Minimal impact on resource availability.	System sabotaged causing significant disruption to noncritical resources. System may not be easily recoverable even with suitable backups.	Sabotage crashes a critical system and leaves it unrecoverable
Compromise			
Application/Service	Does not involve sensitive data	Users computers become compromised after using the service. No sensitive data involved.	Results in data leakage which is sensitive in nature
System	Does not involve sensitive data	A compromised system is used to gain access to other systems, resulting in numerous compromised hosts. None of the systems contain sensitive data.	Results in data leakage which is sensitive in nature
User Account	Account has no elevated privileges to sensitive resources	The compromised account is used to gain access on a system(s) containing non-sensitive information, possibly attacking other systems	The compromised account is used to gain access on a system(s) containing sensitive information, possibly attacking other systems
Exposure			
Human/programming error	An error which has the potential to divulge non-sensitive information that should not be accessed	An error which results in non-sensitive data being accessed/viewed by unauthorized persons	An error which results in sensitive data being accessed/viewed by unauthorized persons (data leak)

Laptop, device, media, paper loss/theft	Media does not contain sensitive information	Media does contain sensitive information and strong encryption is used to protect data	Sensitive information and/or passwords to systems containing sensitive information is stored on the stolen/lost media and is potentially accessible
Misuse/Unauthorized access	Abusing or gaining access to non-sensitive information/resources. Investigation is needed to verify if other resources are compromised.	Abusing or gaining access to non-sensitive information/resources with multiple accounts. Investigation is needed to verify if other resources are compromised.	Abusing or gaining access to sensitive information/resources. Investigation is needed to verify if other resources are compromised. Investigation is needed to verify the extent of the information dissemination
Scams			
Phishing attack impersonating McGill IT	Solutions can be immediately applied to effectively contain the issue	Users have responded to the phishing attempt, releasing personal information. Solutions are not immediate.	Phishing attack that is not easily contained and resulting in widespread compromise of email accounts or accounts with escalated privileges
Social Engineering	Gain unauthorized access to a non-sensitive system	Gain unauthorized access to multiple non-sensitive system(s) and possibly modify data	Gain unauthorized access to highly sensitive system(s) and possibly modify data
Virus/Worm outbreak	Outbreak which can be easily contained and results in a small number of infected hosts ***** REPORTING NOT REQUIRED *****	Outbreak which cannot be easily contained and results in a significant number of infected hosts	Outbreak which cannot be contained and results in a major impact on the network and/or network resources
Vulnerabilities (server-side)	* Vulnerability is discovered for a non-critical service that resides on a non-critical/non-sensitive system. Exploit code may or may not be available. * Mitigating actions exist to secure against a possible compromise of a critical or non-critical system/service. * Mitigating actions exist to secure against a possible compromise of a system containing sensitive information. ***** REPORTING NOT REQUIRED *****	Vulnerability is discovered for either a critical server or a service hosted on a system containing sensitive information. Exploit code may or may not be available. No mitigating actions can be taken to secure against possible compromise.	Vulnerability is discovered for either a critical server or a service hosted on a system containing sensitive information. Exploit code is available. No mitigating actions can be taken to secure against possible compromise.