Information Security Risk Assessment

Contents

MENU

Risk Register

Ready when you are!

Risk Title	Description	Cause	Effect	Owner	Probability	Impact	Inherent Risk
Employee misconfigured cloud environment	Unauthorized parties accessed customer data by connecting through the public internet.	Due to security misconfiguration of their cloud storage environment, for example, configured to allow public access without restriction. Employee inadvertently opens private databases containing customer information to the public internet.	The company exposed to ransom attack, customers at risk of identity theft.	Aleksandar Nenov	Possible	Catastrophic	High
The contractor built 'backdoors' into the software he was commissioned to develop	Hacker exfiltrated the customer data seemingly on an as needed basis.	Software development contractor deliberately built 'backdoors' into the software he was brought in to create on behalf of various retail companies.	Customers experienced financial theft and identity theft.	Igor Gavric	Remote	Catastrophic	Medium
An employee commits access credentials into the source code	Hackers via the stolen credentials gain access to customer information.	Employee inadvertently (or deliberately) inputs access credentials within the source code.	Customers at risk of identity theft as a result of the exposure and the company received significant criticism for their incident response.	Igor Gavric	Possible	Catastrophic	High
Employee exfiltrates customer data and sells it to third parties	Sensitive customer data including credit card numbers exposed to unauthorized parties.	The employee deliberately copied the full complement of customer records motivated by personal financial gain.	Customers at risk of identity theft and financial theft.	Marlon Koch	Remote	Catastrophic	Medium
Actual customer data exposed in test development environment	Employee exposes actual customer data in test development environment.	Employee inputs actual customer data in 'test version' of their website.	Customers received nuisance SMS text messages as a direct result of the exposure.	Igor Gavric	Possible	Catastrophic	High

Control Register

<table>
<tr><th>Control Title</th><th>Objective</th><th>Procedure</th><th>Mitigating</th></tr>
<tr>
<td>Data Protection</td>
<td>To ensure that information receives an appropriate level of protection.</td>
<td>The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data and ensure the privacy and integrity of sensitive information.

1. Deploy approved encryption algorithms and protocols.
2. Verify that cryptographic encryption algorithms and protocols are in place.
3. Assess data to identify sensitive information.
4. Deploy an automated tool on network perimeters that continuously scan for changes in deployed configurations.
5. Move data between networks using secure methods
6. Only allow approved Certificate Authorities (CAs).
7. Perform an annual review of algorithms.
8. Monitor all traffic leaving the organization
9. Define roles and responsibilities related to management.
10. Enforce strict confidentiality agreements with all employees & third-party contractors.</td>
<td>
<table>
<tr><th>Risk</th><th>Owner</th><th>Frequency</th><th>Level</th><th>Type</th><th>Timing</th></tr>
<tr><td>Employee exfiltrates customer data and sells it to third parties</td><td>Marlon Koch</td><td>Ad hoc</td><td>Pervasive</td><td>Manual but IT</td><td>Preventative</td></tr>
<tr><td>The contractor built ‘backdoors’ into the software he was commissioned to develop</td><td>Igor Gavric</td><td>Ad hoc</td><td>Pervasive</td><td>Manual but IT</td><td>Preventative</td></tr>
<tr><td>Employee misconfigured cloud storage environment</td><td>Aleksandar Nenov</td><td>One-off</td><td>Pervasive</td><td>Manual</td><td>Preventative</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr><th>Control Title</th><th>Objective</th><th>Procedure</th><th colspan="6">Mitigating</th></tr>
<tr><td rowspan="4">Control Access Based on the Need to Know</td><td rowspan="4">To control access to information based on a business need.</td><td rowspan="4">The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, and systems) according to the formal determination of which persons, computers and applications have a need and right to access these critical assets based on an approved classification.

1. Locate any sensitive information on separated storage.
2. Enforce detailed audit logging for access.
3. Segment the network based on the trust levels.</td><td>Risk</td><td>Owner</td><td>Frequency</td><td>Level</td><td>Type</td><td>Timing</td></tr>
<tr><td>Actual customer data exposed in a test development environment</td><td>Igor Gavric</td><td>Ad hoc</td><td>Transactional</td><td>Manual but IT</td><td>Preventative</td></tr>
<tr><td>Employee exfiltrates customer data and sells it to third parties</td><td>Marlon Koch</td><td>Ad hoc</td><td>Pervasive</td><td>Manual but IT</td><td>Preventative</td></tr>
<tr><td colspan="6"></td></tr>
</table>

<table>
<tr><th>Control Title</th><th>Objective</th><th>Procedure</th><th colspan="6">Mitigating</th></tr>
<tr><td rowspan="4">Maintenance, Monitoring, and Analysis of Audit Logs</td><td rowspan="4">To detect unauthorized information processing activities.</td><td rowspan="4">Collect, manage and analyze audit logs of events that could help detect, understand or recover from an attack.

1. Include at least two synchronized time sources of logging.
2. Validate audit log settings for each system.
3. Ensure that all systems that store logs have adequate storage.
4. Develop a log retention policy to make sure that all logs would be preserved
5. Have Info security personnel.
6. Configure network boundary devices (IPS and IDS)
7. For all systems, ensure that logs are written.
8. Monitor for service creation events and enable process tracking.
9. Ensure that the log collection system does not lose events.</td><td>Risk</td><td>Owner</td><td>Frequency</td><td>Level</td><td>Type</td><td>Timing</td></tr>
<tr><td>Actual customer data exposed in a test development environment</td><td>Igor Gavric</td><td>Weekly</td><td>Monitoring</td><td>Manual but IT</td><td>Detective</td></tr>
<tr><td>Employee exfiltrates customer data and sells it to third parties</td><td>Marlon Koch</td><td>Weekly</td><td>Monitoring</td><td>Manual but IT</td><td>Detective</td></tr>
<tr><td>The contractor built ‘backdoors’ into the software he was commissioned to develop</td><td>Igor Gavric</td><td>Daily</td><td>Monitoring</td><td>Manual but IT</td><td>Detective</td></tr>
</table>

<table>
<tr><th>Control Title</th><th>Objective</th><th>Procedure</th><th colspan="6">Mitigating</th></tr>
<tr><td rowspan="5">Security Skills Assessment and Appropriate Training to Fill Gaps</td><td rowspan="5">To ensure that all employees, contractors and third-party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their regular work, and to reduce the risk of human error.</td><td rowspan="5">For all functional roles in the organization prioritizing those mission critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support the defense of the enterprise; develop and execute an integrated plan to assess, identify gaps and remediate through policy, organizational planning, training and awareness programs.

1. Perform gap analysis to see which skills employees need.
2. Deliver training to fill the skills gap.
3. Implement an online security awareness program.
4. Validate and improve awareness levels.
5. Use security skills assessments.</td><td>Risk</td><td>Owner</td><td>Frequency</td><td>Level</td><td>Type</td><td>Timing</td></tr>
<tr><td>Actual customer data exposed in a test development environment</td><td>Igor Gavric</td><td>Annually</td><td>Pervasive</td><td>Manual</td><td>Corrective</td></tr>
<tr><td>Employee exfiltrates customer data and sells it to third parties</td><td>Marlon Koch</td><td>Annually</td><td>Pervasive</td><td>Manual</td><td>Corrective</td></tr>
<tr><td>Employee commits access credentials into source code</td><td>Igor Gavric</td><td>Annually</td><td>Pervasive</td><td>Manual</td><td>Corrective</td></tr>
<tr><td>Employee misconfigured cloud storage environment</td><td>Aleksandar Nenov</td><td>Annually</td><td>Pervasive</td><td>Manual</td><td>Corrective</td></tr>
</table>

<table>
<tr><th>Control Title</th><th>Objective</th><th>Procedure</th><th colspan="6">Mitigating</th></tr>
<tr><td rowspan="5">Application Software Security</td><td rowspan="5">To maintain the security of application system software and information.</td><td rowspan="5">Manage the security lifecycle of all in house developed and acquired software to prevent, detect and correct security weaknesses.

1. For all acquired application software, check for vulnerabilities
2. Protect web applications by deploying web application firewalls.
3. Test in-house-developed and third-party procured software for vulnerabilities
4. Do not display system error messages.
5. Maintain separate environments for production and development
6. Test in-house-developed web and other application.</td><td>Risk</td><td>Owner</td><td>Frequency</td><td>Level</td><td>Type</td><td>Timing</td></tr>
<tr><td>Actual customer data exposed in a test development environment</td><td>Igor Gavric</td><td>Daily</td><td>Pervasive</td><td>Manual</td><td>Preventative</td></tr>
<tr><td>Employee commits access credentials into source code</td><td>Igor Gavric</td><td>Daily</td><td>Monitoring</td><td>Manual but IT</td><td>Preventative</td></tr>
<tr><td>The contractor built ‘backdoors’ into the software he was commissioned to develop</td><td>Igor Gavric</td><td>Daily</td><td>Monitoring</td><td>Manual but IT</td><td>Detective</td></tr>
<tr><td>Employee misconfigured cloud storage environment</td><td>Aleksandar Nenov</td><td>Daily</td><td>Monitoring</td><td>Automated</td><td>Detective</td></tr>
</table>

Control Title	Objective	Procedure	Mitigating					
			Risk	Owner	Frequency	Level	Type	Timing
Malware Defenses	To protect the integrity of software and information.	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action. 1. Employ automated anti-malware software that monitors continuously. 2. Configure laptops, workstations, and servers with anti-malware solution 4. Configure systems so that they automatically update. 5. Scan and block all e-mail attachments. 6. Limit the use of external devices. 7. Implement an incident response process.	The contractor built 'backdoors' into the software he was commissioned to develop	Igor Gavric	Daily	Pervasive	Automated	Preventative

Control Title	Objective	Procedure	Mitigating					
			Risk	Owner	Frequency	Level	Type	Timing
Code Review	Four-eyes principle for all written code, including code written by third-party contractors.	Developers are paired and review each others code before a feature branch is merged into develop. Code review is tracked through JIRA and pull requests. Third-party contractors are assigned a developer that reviews their code prior to being merged into develop.	The contractor built 'backdoors' into the software he was commissioned to develop	Igor Gavric	Daily	Transactional	Manual	Preventative

Risks Matrix

Risk: Employee misconfigured cloud environment

Description	Cause	Effect	In. Imp.	In. Prob.	In. Risk	Res. Imp.	Res. Prob.	Res. Risk
Unauthorized parties accessed customer data by connecting through the public internet.	Due to security misconfiguration of their cloud storage environment, for example, configured to allow public access without restriction. Employee inadvertently opens private databases containing customer information to the public internet.	The company exposed to ransom attack, customers at risk of identity theft.	Catastrophic	Possible	High	Catastrophic	Remote	Medium

Control suite

Control Title	Owner	Frequency	Level	Type	Timing	Mitigation	Design	Performance	Effectiveness
Security Skills Assessment and Appropriate Training to Fill Gaps	Aleksandar Nenov	Annually	Pervasive	Manual	Corrective	High	Effective	Effective	Effective
Application Software Security	Aleksandar Nenov	Daily	Monitoring	Automated	Detective	High	Effective	Effective	Effective
Data Protection	Aleksandar Nenov	One-off	Pervasive	Manual	Preventative	High	Effective	Effective	Effective

Risk: Contractor built ‘backdoors’ into the software he was commissioned to develop

Description	Cause	Effect	In. Imp.	In. Prob.	In. Risk	Res. Imp.	Res. Prob.	Res. Risk
Hacker exfiltrated the customer data seemingly on an as needed basis.	Software development contractor deliberately built ‘backdoors’ into software he was brought in to create on behalf of various retail companies.	Customers experienced financial theft and identity theft.	Catastrophic	Remote	Medium	Catastrophic	Extremely Remote	Medium

Control suite

Control Title	Owner	Frequency	Level	Type	Timing	Mitigation	Design	Performance	Effectiveness
Malware Defenses	Igor Gavric	Daily	Pervasive	Automated	Preventative	High	Effective	Effective	Effective
Application Software Security	Igor Gavric	Daily	Monitoring	Manual but IT	Detective	High	Effective	Effective	Effective
Maintenance, Monitoring, and Analysis of Audit Logs	Igor Gavric	Daily	Monitoring	Manual but IT	Detective	High	Effective	Effective	Effective
Data Protection	Igor Gavric	Ad hoc	Pervasive	Manual but IT	Preventative	High	Effective	Effective	Effective
Code Review	Igor Gavric	Daily	Transactional	Manual	Preventative	High	Effective	Effective	Effective

Risk: Employee commits access credentials into the source code

Description	Cause	Effect	In. Imp.	In. Prob.	In. Risk	Res. Imp.	Res. Prob.	Res. Risk
Hackers via the stolen credentials gain access to customer information.	Employee inadvertently (or deliberately) inputs access credentials within the source code.	Customers at risk of identity theft as a result of the exposure and the company received significant criticism for their incident response.	Catastrophic	Possible	High	Catastrophic	Remote	Medium

Control suite

Control Title	Owner	Frequency	Level	Type	Timing	Mitigation	Design	Performance	Effectiveness
Application Software Security	Igor Gavric	Daily	Monitoring	Manual but IT	Preventative	High	Effective	Effective	Effective
Security Skills Assessment and Appropriate Training to Fill Gaps	Igor Gavric	Annually	Pervasive	Manual	Corrective	High	Effective	Effective	Effective

Risk: Employee exfiltrates customer data and sells it to third parties

Description	Cause	Effect	In. Imp.	In. Prob.	In. Risk	Res. Imp.	Res. Prob.	Res. Risk
Customer data including credit card numbers exposed to unauthorized parties.	The employee deliberately copied the full complement of customer records motivated by personal financial gain.	Customers at risk of identity theft and financial theft.	Catastrophic	Remote	Medium	Catastrophic	Remote	Medium

Control suite

Control Title	Owner	Frequency	Level	Type	Timing	Mitigation	Design	Performance	Effectiveness
Security Skills Assessment and Appropriate Training to Fill Gaps	Marlon Koch	Annually	Pervasive	Manual	Corrective	High	Partially effective	Effective	Partially effective
Maintenance, Monitoring, and Analysis of Audit Logs	Marlon Koch	Weekly	Monitoring	Manual but IT	Detective	High	Partially effective	Effective	Partially effective
Control Access Based on the Need to Know	Marlon Koch	Ad hoc	Pervasive	Manual but IT	Preventative	High	Effective	Effective	Effective
Data Protection	Marlon Koch	Ad hoc	Pervasive	Manual but IT	Preventative	High	Effective	Effective	Effective

Risk: Actual customer data exposed in a test development environment

Description	Cause	Effect	In. Imp.	In. Prob.	In. Risk	Res. Imp.	Res. Prob.	Res. Risk
Employee exposes actual customer data in test development environment.	Employee inputs actual customer data in 'test version' of their website.	Customers received nuisance SMS text messages as a direct result of the exposure.	Catastrophic	Possible	High	Catastrophic	Remote	Medium

Control suite

Control Title	Owner	Frequency	Level	Type	Timing	Mitigation	Design	Performance	Effectiveness
Application Software Security	Igor Gavric	Daily	Pervasive	Manual	Preventative	Medium	Partially effective	Effective	Partially effective
Security Skills Assessment and Appropriate Training to Fill Gaps	Igor Gavric	Annually	Pervasive	Manual	Corrective	Medium	Partially effective	Effective	Partially effective
Maintenance, Monitoring, and Analysis of Audit Logs	Igor Gavric	Weekly	Monitoring	Manual but IT	Detective	High	Partially effective	Effective	Partially effective
Control Access Based on the Need to Know	Igor Gavric	Ad hoc	Transactional	Manual but IT	Preventative	High	Effective	Effective	Effective

Risk Rating Definitions

Impact

Rating	Definition
Catastrophic	>20 customers affected. Significant national and international media coverage of event lasting for months. Significant regulatory implications and censure will require significant remediation activity to be undertaken. Large-scale changes to operations or control environment required.
Critical	10-20 customers affected. Significant local media coverage of event lasting for weeks, possible limited national coverage. Some regulatory implications or criticism will require remediation activity to be undertaken. Large changes to operations or control environment required.
Significant	2-10 customers affected. Limited local media coverage of event lasting for days. Limited regulatory implications or censure, possible re-work/remediation. Some changes to operations or control environment required.
Important	<2 customers affected. No media coverage of the event. No regulatory implications or censure. No changes to operations or control environment required.

Probability

Rating	Definition
Likely	Will occur within the next 1-6 months.
Possible	Will occur within the next year.
Remote	Will occur within the next 5 years.
Extremely Remote	Will occur within the next 10 years.

Information Security Risk Assessment Completion

Date	Completed by:	Reviewed and Approved by:
20.05.2019	Marlon Koch	
12.12.2019	Marlon Koch	
26.07.2020	Marlon Koch	

MENU Technologies AG · Dammstrasse 19 · 6301 Zug, Switzerland · +41 41 723 2041 · hello@menu.app