



ROCHESTER INSTITUTE OF TECHNOLOGY

CSEC-603: ENTERPRISE SECURITY

---

# Cybersecurity Report of Intel Corporation

---

*Prepared For:*

**Bill Stackpole**

Professor

Department of Computing

Security

*Prepared By :*

**Mohammad Saidur Rahman**

Graduate Student

Department of Computing

Security

27 April 2018

# Executive Summary

Intel Corporation is one of the biggest semiconductor manufacturing enterprises of this world. In this paper, we investigate various issues related to cybersecurity of Intel Corporation such as risks and vulnerabilities assessment, identifying controls to mitigate those risks and vulnerabilities, and proposing budgets to deploy those controls. To find the potential vulnerabilities of Intel Corporation, we carefully analyze information published in the Intel website such as the financial documents of the last four quarters of Intel, investors information, supplier information, security policies, password policies, supply chain information, and communities support portal. We also investigate exciting news (i.e., meltdown, spectre, and SGXPECTRE) from various sources. Any significant information from the financial information cannot be related to any vulnerability. However, the password policy and account login information give compelling insight to attack. It turns out; a persistent attacker can take advantage of this kind of vulnerability and break the accounts of the stakeholders such as employee, supplier, the community supporter of Intel. Besides, there is a new attack published that can exploit the software guard extensions (SGX) environment and reveal information from that. The vulnerabilities are classified into two groups: enterprise related, and product related. The controls are identified considering those two sections of vulnerabilities. The controls are recommended based on preventive, detective, forensic, and audit. The identified controls can act as the shields against the identified vulnerabilities. The objective of those identified controls is to reduce the risks and probability of being attacked. Budgeting is a hard task for cybersecurity as the people involved in financing may not appreciate the fact that investing cybersecurity may not give us quick return. The best we can do is to ensure that we have taken place all the measures to reduce the impact of the attack. Also, we try to ensure that we can respond to the attacks as soon as possible. However, the goal of budgeting for cybersecurity is to ensure that we have enough money to deploy a potentially perfect defense mechanism in Intel Corporation. For that purpose, we have prepared three budgets that take account of the minimalistic budget, medium cost budget, and high-cost budget. In the next section of this document, we describe the risks and the vulnerabilities of Intel Corporation. Afterward, we describe the controls that may help to mitigate the risks. Finally, we describe the budgets and conclude.

# Table of Contents

<b>List of Figures</b>	<b>iii</b>
<b>List of Tables</b>	<b>iii</b>
<b>1 Risk &amp; Vulnerabilities of Intel Corp.</b>	<b>1</b>
1.1 Enterprise related Potential Vulnerabilities . . . . .	1
1.1.1 Breaking the Password (Weak Password Policy) . . . . .	1
1.1.2 Trying to Access the Supplier Site . . . . .	1
1.1.3 Illustration of the Attack . . . . .	2
1.2 Product related Potential Vulnerability(ies) . . . . .	2
1.2.1 Intel SGX (Software Guard Extensions) . . . . .	2
1.2.2 Bug Bounty Program . . . . .	2
1.3 Probability versus Impact Matrix . . . . .	3
<b>2 Cybersecurity Controls of Intel Corp.</b>	<b>4</b>
2.1 Controls for Enterprise Related Vulnerabilities . . . . .	5
2.2 Controls for Product Related Vulnerabilities . . . . .	6
2.3 Controls in the Big Picture . . . . .	7
<b>3 Cybersecurity Budget of Intel Corp.</b>	<b>8</b>
3.1 Budget . . . . .	8
3.2 Low-Cost Budget . . . . .	10
3.2.1 Analysis of the Low Cost Budget . . . . .	12
3.3 Medium Cost Budget . . . . .	13
3.3.1 Analysis of Medium Cost Budget . . . . .	13
3.4 High-Cost Budget . . . . .	15
3.4.1 Analysis of High Cost Budget . . . . .	15
3.5 Analysis of Three Budgets . . . . .	17
<b>4 Conclusion</b>	<b>18</b>
<b>References</b>	<b>19</b>
<b>Appendix A Screen shot of the Supplier Email</b>	<b>21</b>

## List of Figures

1	Probability versus Impact Matrix . . . . .	3
2	Cybersecurity Controls. . . . .	4
3	Controls for Enterprise related Vulnerabilities. . . . .	5
4	Controls for Product related Vulnerabilities. . . . .	7
5	Low Cost Budget . . . . .	11
6	Low Cost Breakdown. . . . .	12
7	Medium Cost Breakdown. . . . .	13
8	Medium Cost Budget. . . . .	14
9	Medium Cost Breakdown. . . . .	15
10	High Cost Budget. . . . .	16
11	Analysis of Three Budgets. . . . .	17

## List of Tables

1	<i>Control in the Big Picture.</i> . . . . .	8
2	<i>Required People for the Controls.</i> . . . . .	9
3	<i>Required Tools for the Controls.</i> . . . . .	10
4	<i>Annual per Employee Cost in Low Cost Budget.</i> . . . . .	12
5	<i>Annual per Employee Cost in Medium Cost Budget.</i> . . . . .	13
6	<i>Annual per Employee Cost in High Cost Budget.</i> . . . . .	15

# 1 Risk & Vulnerabilities of Intel Corp.

Though it is difficult to find out potential vulnerabilities from the publicly faced documents of an organization, it is surprising that some interesting potential vulnerabilities are discovered. The vulnerabilities are categorized as product related vulnerabilities and enterprise related vulnerabilities.

## 1.1 Enterprise related Potential Vulnerabilities

### 1.1.1 Breaking the Password (Weak Password Policy)

There is a potential vulnerability in the password policy of Intel Corporation. The password policy of Intel seems very weak compared to the current best practices. In the current scenario, the minimum password length of a secure password should be 16 (as we are aware of this from the lecture of Professor Stackpole). However, Intel enforces minimum password to be 8 and the maximum password to be 15 ([Intel, 2018d](#)). Intel also gives ten failed login attempts at a time. The account is locked out after ten failed login attempts. A user can try to login after 10 minutes. Someone outside of the organization can easily be a member of their community support. The password policy is same for all the users (i.e., employees, and outside people) of their web interface. A persistent attacker knowing this policy can invest time to break the password of a legitimate user. The information that is available to an attacker is as follows:

- Minimum and maximum password length
- Format of allowed password
- Account lockout policy

An attacker has the scope to try 60 passwords in an hour. A persistent attacker can try hour after hour finding the right match.

### 1.1.2 Trying to Access the Supplier Site

If an attacker opens an account to the Intel community support, the attacker can use the same login information to try to access the supplier site ([Intel, 2018b](#)). The supplier site of Intel contains lots of sensitive information about their supply chain

and shipments. If an attacker is persistent, the attacker can target a supplier and invest time to figure out the password.

As an attacker needs only one point of entry to the infrastructure, the attacker can target employees, general users, suppliers of Intel and potentially break into an account with a sufficient amount of effort and time.

### **1.1.3 Illustration of the Attack**

We created an account in the community support account of Intel. We used the same credential to access their supplier account. We requested access to their supplier account. Though we do not know yet whether we are authorized to access their supplier site, we can get some email containing the information that we are not supposed to get. A screenshot of the email is given in [Appendix A](#).

## **1.2 Product related Potential Vulnerability(ies)**

### **1.2.1 Intel SGX (Software Guard Extensions)**

All the current Intel processor has a feature called software guard extensions (SGX) that is aimed to execute code securely inside an isolated environment called enclave. Intel claims that it is the most secure environment to perform any sensitive operation and it is even isolated from the operating systems level. However, there is a recent publication by Chen et al. ([Chen et al., 2018](#)) that shows that it is possible to exploit the SGX environment. They named this new type of attack as SGXPECTRE that can exploit under the assumption that an attacker has access to the machine. This vulnerability can be a big shock for Intel after the meltdown and specter. Intel needs to rebuild and redeploy the updated development kit to protect the SGX ([Chirgwin, 2018](#)). Though Intel mentioned publishing a patch for the vulnerability with March 16, to our best knowledge they have not done that ([Cimpanu, 2018](#)).

### **1.2.2 Bug Bounty Program**

Though the patches of Meltdown and Spectre are now publicly available right now, they are apparently degrading the current performance of the machines ([Intel, 2018c](#)). It is a significant indicator that there can be other vulnerabilities in the Intel hardware. Moreover, this assumption has become stronger seeing the Intel's

bug bounty program. Intel invited security researchers to work on finding new vulnerabilities in their products, and they have also offered a monetary reward for successful findings. That gives an attacker intuition about the fact that Intel products might have undiscovered vulnerabilities. Though we cannot ensure this fact with high confidence, at the same time, we cannot ignore that either.

### 1.3 Probability versus Impact Matrix

Considering the above vulnerabilities, the probability and risk matrix is given in Figure 1).

		Impact		
		Low	Medium	High
Probability of Occurrence	High			<b>Enterprise Related Potential Vulnerabilities (Password Policy)</b>
	Medium			<b>Product related Potential Vulnerability(ies)</b>
	Low			

Figure 1: Probability versus Impact Matrix

## 2 Cybersecurity Controls of Intel Corp.

Information security controls or cybersecurity controls enable an organization to understand how it should respond to specific vulnerabilities or risks. In other words, controls define what the reaction of a particular action of an attacker is. For example, if an attacker breaks into an administrative account, the organization respond by isolating that machine from the primary network. The possible actions against an attacker will give the organization relative level of transparency of their capability. The controls should be documented based on the risks or vulnerabilities identified. The principal objective of controls is to ensure the CIA (confidentiality, integrity, and availability) triad. The reason is that the vulnerabilities are identified based on the CIA triad. Hence, the control measures also aim to protect the CIA.

There are different frameworks for security controls. For example, controls provided by the center for information security (CIS), NIST SP 800-53 (security and privacy controls for federal information systems and organizations), and Council on Cyber Security (Critical Security Controls for Effective Cyber Defense v5). However, the controls can focus either on physical security, technical security, and administrative (Northcutt, 2018), or all three divisions simultaneously.



Figure 2: Cybersecurity Controls.

Controls are grouped into four categories (see Figure 2): forensic, audit, detective, and preventive (Donaldson et al., 2015). Preventive controls will help to block the incidents from occurring, and detective controls will help to detect any incident



occurring, forensic controls will help to collect the logs of events and create artifacts, audit controls will try to ensure whether the other three controls are working in the way it is supposed to.

## 2.1 Controls for Enterprise Related Vulnerabilities

		Vulnerabilities	
		Enterprise Related Vulnerabilities – Password Policies	Challenges to Deploy
Controls	Preventive	<ul style="list-style-type: none"> <li>Deploying New Password Policies by removing all the shortcoming of the existing one.</li> </ul>	Will cause additional cost from the policy making to the dissemination.
		<ul style="list-style-type: none"> <li>Separating the account types completely (i.e. employee accounts, community engagement accounts, and supplier accounts).</li> </ul>	May be difficult if they do not have the infrastructure or their infrastructure does not support this.
		<ul style="list-style-type: none"> <li>Separate Policies for different account types.</li> </ul>	Management can be hard.
		<ul style="list-style-type: none"> <li>Reducing the number of login attempts.</li> </ul>	Relatively easy
		<ul style="list-style-type: none"> <li>Enforcing the least password length of sixteen characters with a combination of numbers, uppercase and lowercase letters, and symbols.</li> </ul>	Some people may not be comfortable with this.
		<ul style="list-style-type: none"> <li>Increasing the account lockout time.</li> </ul>	Some people might be against. If legitimate users enter password by mistake and <u>have to</u> wait for a long time to retry, they may not find this comfortable.
	Detective	<ul style="list-style-type: none"> <li>Monitoring the accounts. *</li> <li>Using SIEM (Security Information and Event Management). *</li> <li>Using IDS (Intrusion Detection System). *</li> <li>Continuous Vulnerability Assessment *</li> </ul>	*If they do not already have those. Additional cost is required, New people are required.
Forensic	<ul style="list-style-type: none"> <li>Keeping Logs of the login events (i.e. failure, success, number of attempts) **</li> <li>Keeping Logs of critical accounts (i.e. accounts with weak passwords) **</li> </ul>	** If they do not already do those. Logging is hard because it requires expertise to define what is normal and what is abnormal.	
Audit	<ul style="list-style-type: none"> <li>✓ Periodic auditing to ensure that all the accounts are maintaining the existing policies. ***</li> <li>✓ Ensuring the access privilege is used by the authorized personnel.</li> <li>✓ Investigating the reasons of the failed login attempts. ***</li> </ul>	*** If they are not already doing that.	

Figure 3: Controls for Enterprise related Vulnerabilities.

Before going to the details of the controls against enterprise related vulnerabilities, the brief of the vulnerabilities is presented below:

- Weak password policy
- Weak password length
- Number of login attempts is higher
- Account lockout policy is weak
- Sam policy for the employee accounts, community engagement accounts, and suppliers accounts.

Considering the vulnerabilities, the potential controls are presented in the [Figure 3](#).

The preventive controls specified in [Figure 3](#) will help to prevent the vulnerabilities completely. Intel Corporation may opt to choose preventive control. In that case, the detective, forensic, and audit controls should be implemented very tightly so that any suspicious events can be detected, logged, and analyzed. The goal should be to identify the attacker and prevent the suspicious actions.

## 2.2 Controls for Product Related Vulnerabilities

There are two potential vulnerabilities related to Intel products identified in [Section 1.2](#) of this paper.

- Intel SGX (Software Guard Extensions) ([Chen et al., 2018](#)).
- Bug Bounty Program ([Intel, 2018c](#)).

In addition to those, we also want to consider the Specter and Meltdown vulnerabilities ([Cimpanu, 2018](#)). Considering the vulnerabilities, the controls are recommend in [Figure 4](#).

Intel may experience a significant amount of financial loss because of the product-related vulnerabilities. These kinds of vulnerabilities impact the customers. The customers may lose trust in their products. Hence, Intel should respond quickly and make the patch before any severe damage happens.

Controls	Vulnerabilities		Challenges to Deploy
	Product Related Vulnerabilities		
	<b>Preventive</b>	<ul style="list-style-type: none"> <li>• Replacing the Product *</li> <li>• Deploying the patch as soon as possible.</li> <li>• Extensive research to find possible vulnerabilities of the products before releasing.</li> </ul>	Replacing the product may not be realistic as it will cost lot of money.
	<b>Detective</b>	<ul style="list-style-type: none"> <li>• Continuous assessment of the products (not only the SGX, rather all the products). **</li> <li>• Developing a Hardware Hacking Team who can continuously try to find the ways to break the products or do harm with those products.</li> </ul>	** If they are not already doing that.
	<b>Forensic</b>	<ul style="list-style-type: none"> <li>• Keeping logs of the impact of the vulnerabilities.</li> </ul>	
<b>Audit</b>	<ul style="list-style-type: none"> <li>• Ensuring all the other controls are working properly.</li> </ul>		

Figure 4: Controls for Product related Vulnerabilities.

### 2.3 Controls in the Big Picture

All the four types of controls may not always be feasible for all kinds vulnerabilities. Some types of controls are critical, and some types of controls are non-critical in some vulnerabilities. The critical and non-critical controls (regarding the four types of the controls) to deal with the two types of vulnerabilities are given in [Table-1](#). The red box indicates critical, the yellow box indicates non-critical, and the orange box indicates somewhat more than non-critical but less than critical.

Table 1: *Control* in the Big Picture.

Vulnerabilities	Controls			
	Preventive	Detective	Forensic	Audit
<b>Enterprise Related Vulnerabilities</b>	Critical, and Strongly Recommended	May not solve the problem completely	Noncritical	Noncritical
<b>Product related Vulnerabilities</b>	- Replacing is not easy as it involves a lot of money. Developing patch immediately is crucial	Detection is very critical, otherwise attacker will keep damaging	Noncritical	Noncritical

### 3 Cybersecurity Budget of Intel Corp.

#### 3.1 Budget

Cybersecurity budget can be made based on different criteria such as the control mechanisms to combat the vulnerabilities of an organization, the assets that need protection from being hacked. The impacts of cybersecurity on the resources of an organization are challenging to assess (Davis et al., 2016). However, most of the budget plan may focus on minimizing cost and maximizing the return on investment. It is no different in case of cybersecurity budget (Force and Initiative, 2013). One approach to preparing the cybersecurity budget can be hierarchical decomposition and requisition such as parent and child relationship (Davis et al., 2016). In this approach, the child activities are completed first to start the parent activities. For example, to mitigate the brute force attack, the password policies are made very strong.

In the process of making the cybersecurity budget, some strategies can be thought beforehand. The strategies will help to determine what the goal is. For example, minimizing exposure, neutralizing attacks, and accelerating the recovery process. The budget objective is to make an active cyber defense such that an organization can minimize the loss of any attack and reduce the probability of the attack (Donaldson et al., 2015).

The cybersecurity budget can be prepared based on the controls that are considered to combat specific vulnerabilities in [Section 1](#). To do that, the first thing an organization needs is skilled people. Other essential elements are tools, technologies, processes, and policies.

We will consider three types of budget schemes: minimal, medium, and high cost. The minimal budget scheme will include the resources that cannot be omitted by any means. The medium cost budget will include almost everything considering the constraint of the organization. Moreover, the high-cost budget will be made taking account of all the actions we can take and all the resources we can deploy. However, the recent study shows that even though the cost of cybersecurity is getting increased, it is still difficult to get the qualified people for the job ([Security, 2018](#)). The critical issue of budgeting would be to find the right people ([ISACA, 2018](#)) for the right job. In our budgeting, we first consider *people* resource (see [Table-2](#)) for that reason.

Table 2: *Required People for the Controls.*

<b>Resource</b>	<b>Roles</b>	<b>Quantity</b>
<b>People</b>	Compliance	5
	Policy	2
	Incident Response	5
	Security Auditor	2
	Forensic Specialist	5
	Researcher	20
	Malware Engineer	3
	SOC Response	3
	Lawyer	2
		<b>Total Number of People Required</b>

As we can see from [Table-1](#) that, some controls are critical, and some controls are non-critical. We prepare budget considering this criticality factors. We have categorized the people (see [Table-2](#)) needed for the controls that are identified. In addition to that, we identify the tools (see [Table-3](#)) , and techniques we will need.

Table 3: *Required Tools for the Controls.*

Resource	Name of the Tool	Quantity
<b>Tools</b>	SIEM	1
	IDS	1
	IPS	1
	Desktop Computer	5
	Laptop Computer	10
	Forensic Software	10
	Log Storage	1
	Backup Storage	1
	Server Hardware	3
	<b>Total Number of Tools Required</b>	<b>33</b>

### 3.2 Low-Cost Budget

In this section, we are proposing a low-cost budget to address the controls of [Section-1](#). As mentioned earlier, the controls are identified to combat two types of vulnerabilities: enterprise related and product related. In the low-cost budget, we need to consider the most critical factors. The risk of the enterprise related vulnerabilities is the weak password policy that might affect the entire organizational chain and may give an attacker scope to take control over the employee accounts, and supplier accounts. Hence, we at least need a person to change the existing policy. In addition to that, we need at least 2 to 3 people to monitor that the employees, community, and the suppliers are following the password policies.

The product-related vulnerabilities are the result of the risk that identified by a group of researchers ([Chen et al., 2018](#)). Intel announced to develop a patch for that vulnerability. However, we expect them to develop an internal research team if they do not have an existing one. The objective of the team will be to find out any product related vulnerabilities that might exist. Moreover, we will need at least a lawyer to maintain all of the legal issues related to cybersecurity. The detailed budget is presented in [Figure 5](#).

## Low-Cost Budget of Intel Corporation for Cybersecurity

Resource(s)	Roles/Name	Quantity	Hourly Rate	Required Hours/Wee	Weekly Cost	Monthly Cost	Per Employee	Annual Total Cost
	Security Manager	1	\$ 48.08	40	\$ 1,923.08	\$ 8,333.33	\$ 100,000.00	\$ 100,000.00
	Compliance	1	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 60,000.00
	Policy	1	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 60,000.00
	Incident Response	1	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 60,000.00
	Security Auditor	1	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 60,000.00
<b>People</b>	Forensic Specialist	1	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 60,000.00
	Researcher	5	\$ 48.08	40	\$ 1,923.08	\$ 8,333.33	\$ 100,000.00	\$ 500,000.00
	Malware Engineer	1	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 60,000.00
	SOC Engineer	1	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 60,000.00
	Lawyer	1	\$ 38.46	40	\$ 1,538.46	\$ 6,666.67	\$ 80,000.00	\$ 80,000.00
	SIEM	1					\$ 200,000.00	\$ 200,000.00
	IDS	1					\$ 2,000.00	\$ 2,000.00
	IPS	1					\$ 2,000.00	\$ 2,000.00
	Desktop	1					\$ 1,500.00	\$ 1,500.00
<b>Tools</b>	Laptop	1					\$ 1,500.00	\$ 1,500.00
	Forensic Software	1					\$ 40,000.00	\$ 40,000.00
	Forensic Storage	1					\$ 5,000.00	\$ 5,000.00
	Log Storage	1					\$ 5,000.00	\$ 5,000.00
	Backup Storage	1					\$ 20,000.00	\$ 20,000.00
	Server Hardware	1					\$ 10,000.00	\$ 10,000.00
<b>Annual Total Cost</b>								<b>\$ 1,387,000.00</b>

Figure 5: Low Cost Budget

### 3.2.1 Analysis of the Low Cost Budget

From the latest annual report, we know that Intel has in total 102,700 employees (Intel, 2018a). We can see from Table-4 that Intel has to spend \$13.50 for an employee annually to implement the security controls of Section-1.

Table 4: Annual per Employee Cost in Low Cost Budget.

Items	
Total Number of Employees	102,700
Annual Cost	\$1,387,000
<b>Yearly Cost Per Employee</b>	<b>\$13.50</b>

We can see from the cost breakdown of the low cost budget (see Figure 6) that the highest expenditures are in people (55%) and in research (25%). 14% of the total cost is proposed to spend on tools and techniques. For the compliance and policy, 3% for each is recommended.

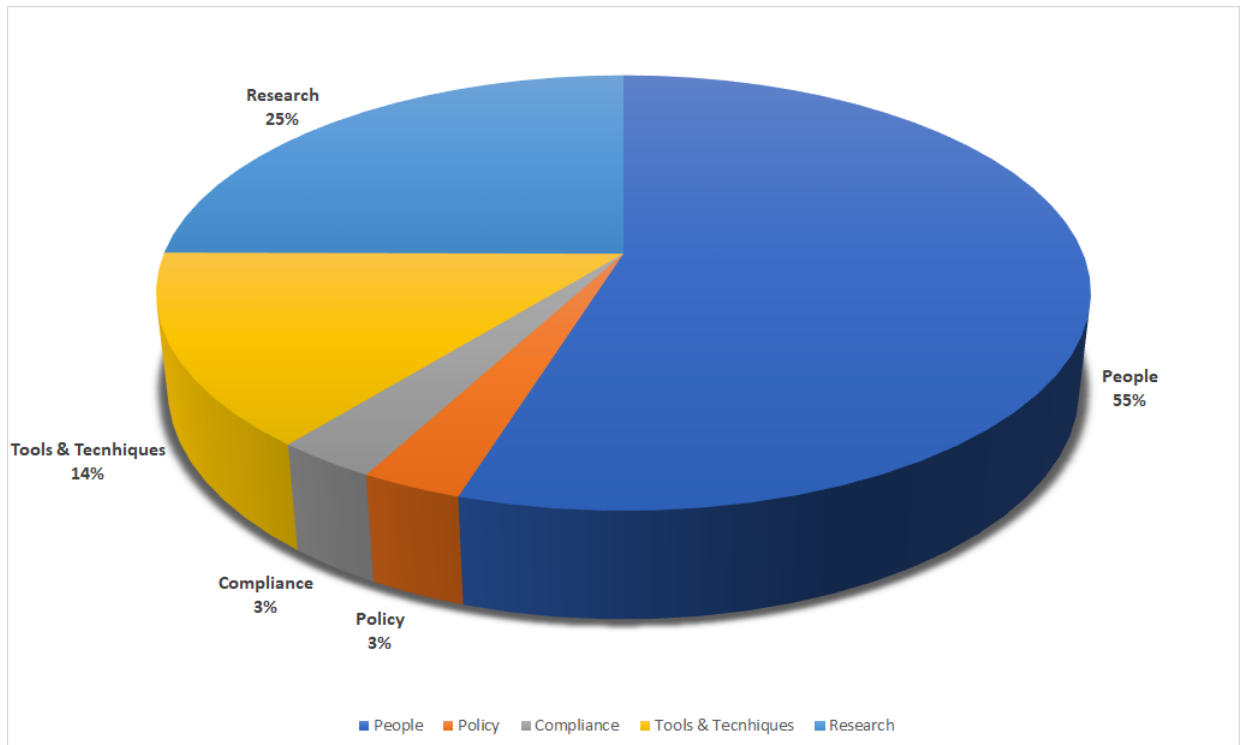


Figure 6: Low Cost Breakdown.



### 3.3 Medium Cost Budget

In the medium cost budget, we will try to address all of the cost just as right maintaining the budget constraints. Medium cost budget is the reflection of the most realistic budget scheme as it tries to close the gap between the needs of Intel corporation and the available money it may be willing to spend. The detailed budget is given in [Figure 8](#).

#### 3.3.1 Analysis of Medium Cost Budget

We can see from [Table-5](#) that Intel has to spend \$114.41 for an employee annually in medium cost budget which is

Table 5: *Annual per Employee Cost in Medium Cost Budget.*

Items	
Total Number of Employees	102,700
Annual Cost	\$11,750,000
<b>Yearly Cost Per Employee</b>	<b>\$114.41</b>
<b>Yearly per Employee Cost Increased by</b>	<b>\$100.91</b>

We can see from the cost breakdown of the medium cost budget (see [Figure 7](#)) that the highest expenditures are in tools and techniques (47%) and in people (34%). 14% of the total cost is proposed to spend on research. For the compliance and policy 4% and 1% respectively is recommended.

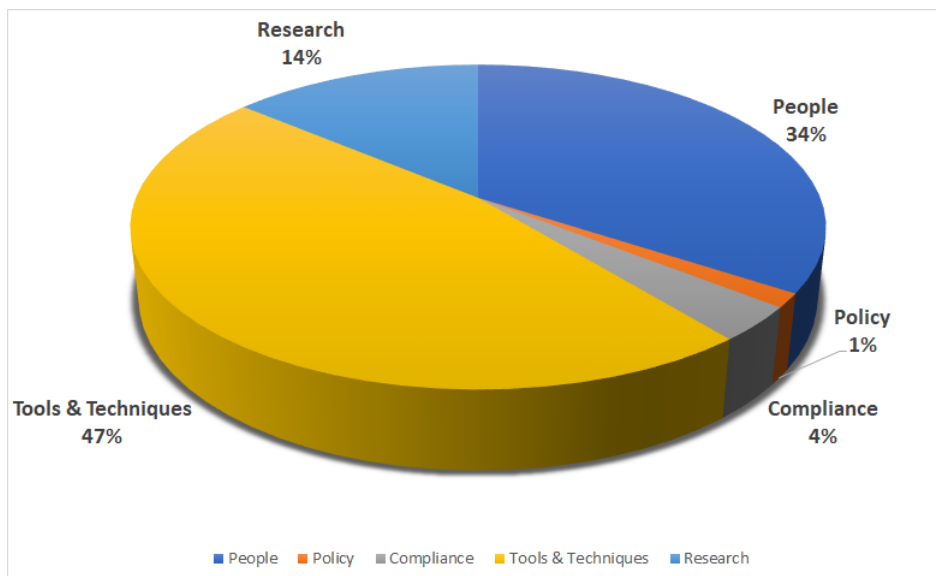


Figure 7: Medium Cost Breakdown.

## Medium-Cost Budget of Intel Corporation for Cybersecurity

Resource(s)	Roles/Name	Quantity	Hourly Rate	Required Hours/Week	Weekly Cost	Monthly Cost	Per Employee Cost	Annual Total Cost
	CISO	1	\$ 72.12	40	\$ 2,884.62	\$ 12,500.00	\$ 150,000.00	\$ 150,000.00
	Security Manager	1	\$ 48.08	40	\$ 1,923.08	\$ 8,333.33	\$ 100,000.00	\$ 100,000.00
	Compliance	5	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 500,000.00
	Policy	2	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 200,000.00
	Incident Response	5	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 500,000.00
	Security Auditor	2	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 200,000.00
	Forensic Specialist	5	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 500,000.00
	Researcher	20	\$ 48.08	40	\$ 1,923.08	\$ 8,333.33	\$ 100,000.00	\$ 2,000,000.00
	Malware Engineer	3	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 300,000.00
	SOC Engineer	3	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 300,000.00
	Lawyer	2	\$ 38.46	40	\$ 1,538.46	\$ 6,666.67	\$ 80,000.00	\$ 200,000.00
	SIEM	1						\$ 200,000.00
	IDS	1						\$ 200,000.00
	IPS	1						\$ 200,000.00
	Desktop	5						\$ 1,000,000.00
	Laptop	10						\$ 2,000,000.00
	Forensic Software	10						\$ 2,000,000.00
	Forensic Storage	1						\$ 200,000.00
	Log Storage	1						\$ 200,000.00
	Backup Storage	1						\$ 200,000.00
	Server Hardware	3						\$ 600,000.00
								<b>Annual Total Cost \$ 11,750,000.00</b>

Figure 8: Medium Cost Budget.

### 3.4 High-Cost Budget

We have prepared the high cost budget thinking that Intel may afford any amount of cost. We added two additional resources that are employee training and supplier training about security awareness. We also increased the number of people and the number of tools required to execute the controls specified. We can see the detailed high cost budget in [Figure 10](#).

#### 3.4.1 Analysis of High Cost Budget

We can see from [Table-5](#) that Intel has to spend \$114.41 for an employee annually in medium cost budget which is

Table 6: *Annual per Employee Cost in High Cost Budget.*

<b>Items</b>	
Total Number of Employees	102,700
Annual Cost	\$18,950,000
<b>Yearly Cost Per Employee</b>	<b>\$184.51</b>
<b>Yearly Increase of Cost from Medium Budget by</b>	<b>\$70.10</b>

Cost breakdown (see [Figure 7](#)) shows that the highest expenditures are in tools and techniques (53%) and in people (31%). 11% of the total cost is proposed to spend on research. For the compliance and policy 2% for each is recommended.

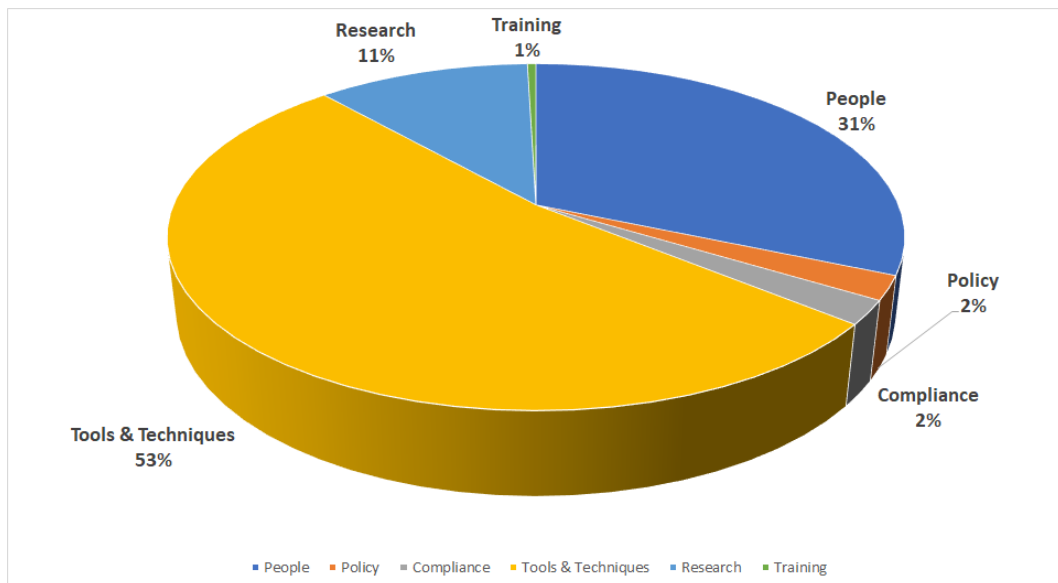


Figure 9: Medium Cost Breakdown.

High-Cost Budget of Intel Corporation for Cybersecurity									
Resource(s)	Roles/Name	Quantity	Hourly Rate	Required Hours/Week	Weekly Cost	Monthly Cost	Per Employee Cost	Annual Total Cost	
	CISO	1	\$ 72.12	40	\$ 2,884.62	\$ 12,500.00	\$ 150,000.00	\$ 150,000.00	
	Security Manager	2	\$ 48.08	40	\$ 1,923.08	\$ 8,333.33	\$ 100,000.00	\$ 200,000.00	
	Compliance	5	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 500,000.00	
	Policy	5	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 500,000.00	
	Incident Response	8	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 800,000.00	
	Security Auditor	3	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 300,000.00	
	Forensic Specialist	5	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 500,000.00	
	Researcher	25	\$ 48.08	40	\$ 1,923.08	\$ 8,333.33	\$ 100,000.00	\$ 2,500,000.00	
	Malware Engineer	5	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 500,000.00	
	SOC Engineer	5	\$ 28.85	40	\$ 1,153.85	\$ 5,000.00	\$ 60,000.00	\$ 500,000.00	
	External Auditor	2	\$ 28.14	41	\$ 1,153.87	\$ 5,000.08	\$ 60,001.00	\$ 200,000.00	
	Lawyer	4	\$ 38.46	40	\$ 1,538.46	\$ 6,666.67	\$ 80,000.00	\$ 400,000.00	
	SIEM	1						\$ 200,000.00	
	IDS	3						\$ 600,000.00	
	IPS	3						\$ 600,000.00	
	Desktop	10						\$ 2,000,000.00	
	Laptop	15						\$ 3,000,000.00	
	Forensic Software	15						\$ 3,000,000.00	
	Forensic Storage	2						\$ 400,000.00	
	Log Storage	2						\$ 400,000.00	
	Backup Storage	3						\$ 600,000.00	
	Server Hardware	5						\$ 1,000,000.00	
Employee Training	Employee Security Awareness							\$ 50,000.00	
Supplier Training	Supplier Security Awareness							\$ 50,000.00	
							Annual Total Cost	\$ 18,950,000.00	

Figure 10: High Cost Budget.

### 3.5 Analysis of Three Budgets

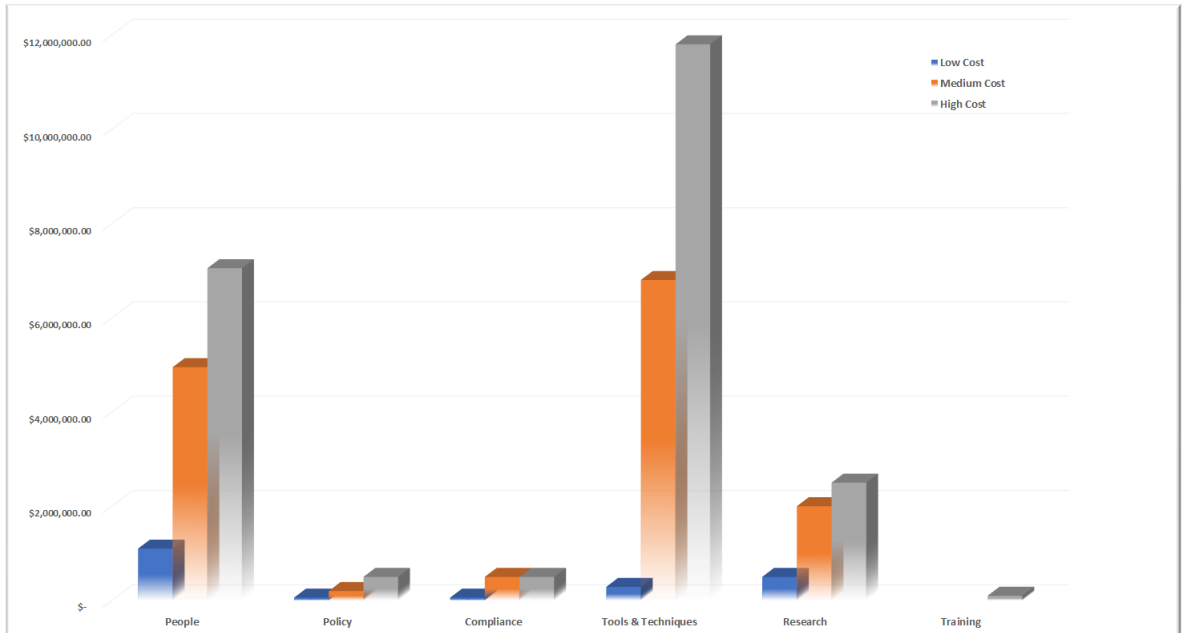


Figure 11: Analysis of Three Budgets.

We can see the analysis of the three proposed budgets in [Figure 11](#). The high cost budget is probably too much high to adopt. On the other hand, we think that medium cost budget is somewhat realistic. The yearly per employee cost is 114.41 in medium cost budget. A large global company like Intel should spend nearly \$100 for each employee for cybersecurity. A large corporation usually spends at least \$10 millions and at best \$50 millions for their security purpose ([Filkins and Hardy, 2016](#)).

In our three budgets the low cost , medium cost, and high cost spending are around \$1.4 millions, \$12 millions, and \$19 millions respectively. Comparing to the industry practices, we can say that our medium cost budget may be suitable. We even cannot rule out the high cost budget.

From the annual report of Intel ([Intel, 2018a](#)), we can see that total expenditure of the year 2017 is \$20.6 billions. If they consider our medium cost budget, the expenditure in cybersecurity would increase by 0.06%. We think that it would be possible for Intel to bear this additional cost.

## 4 Conclusion

Intel corporation should examine the issues of the password policy. With the advancement of attack tools, attacker perception, and reconnaissance capabilities, it would increase the possibility of an attacker to attack the user accounts. Hence, it would be an excellent approach for Intel to rethink their password policy. In addition to that, they should investigate more about their existing products to discover whether there are any vulnerability issues in the products. Intel can consider the deployment of the documented controls so that they can strengthen their existing cyberdefense. Controls are recommended based on the detective, preventive, forensic, and audit issues in mind. The controls are investigated taking account of the two types of vulnerabilities (i.e., enterprise related, and product-related). In the budgeting, to combat the cybersecurity threats, vulnerabilities, and risks, and to address the controls, three types of budgets are recommended: low, medium, and high cost. The budget elements direct the resources that are required to implement the controls specified in the control section. The low-cost budget is not realistic in a sense because it cannot solve the existing cybersecurity challenges. The high-cost budget is also too high for the organization to afford. The medium cost budget is somewhat realistic as it maximizes the deployment of controls. Though cybersecurity budgeting is always an ambiguous issue as the return cannot be seen just in time, we still have to be prepared with the most robust defense mechanism.

## References



- Chen, G., Chen, S., Xiao, Y., Zhang, Y., Lin, Z., and Lai, T. H. (2018). SGXPECTRE Attacks: Leaking enclave secrets via speculative execution. *arXiv preprint arXiv:1802.09085*.
- Chirgwin, R. (2018). Spectre haunts intel’s SGX defense: CPU flaws can be exploited to snoop on enclaves. [https://www.theregister.co.uk/2018/03/01/us\\_researchers\\_apply\\_spectrestyle\\_tricks\\_to\\_break\\_intels\\_sgx/](https://www.theregister.co.uk/2018/03/01/us_researchers_apply_spectrestyle_tricks_to_break_intels_sgx/). Accessed: 2018-03-10.
- Cimpanu, C. (2018). SgxSpectre attack can extract data from Intel SGX Enclaves. <https://www.bleepingcomputer.com/news/security/sgxspectre-attack-can-extract-data-from-intel-sgx-enclaves/>. Accessed: 2018-03-10.
- Davis, J. I., Libicki, M. C., Johnson, S. E., Kumar, J., Watson, M., and Karode, A. (2016). A framework for programming and budgeting for cybersecurity. Technical report, RAND Corporation Santa Monica United States.
- Donaldson, S., Siegel, S., Williams, C., and Aslam, A. (2015). *Enterprise Cybersecurity: how to build a successful cyberdefense program against advanced threats*.
- Filkins, B. and Hardy, G. (2016). IT Security Spending Trends. <https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697>. Accessed: 2018-04-25.
- Force, J. T. and Initiative, T. (2013). Security and privacy controls for federal information systems and organizations. *NIST Special Publication*, 800(53). Accessed: 2018-04-20.
- Intel (2018a). 2017 annual report and form 10-k. [https://s21.q4cdn.com/600692695/files/doc\\_financials/2017/annual/Intel\\_Annual\\_Report\\_Final-3.20.pdf](https://s21.q4cdn.com/600692695/files/doc_financials/2017/annual/Intel_Annual_Report_Final-3.20.pdf). Accessed: 2018-04-25.
- Intel (2018b). Intel supplier. <https://supplier.intel.com/supplierhub/>. Accessed: 2018-04-20.
- Intel (2018c). Intel ® bug bounty program. <https://security-center.intel.com/BugBountyProgram.aspx>. Accessed: 2018-04-20.

- Intel (2018d). Sign in FAQ. <https://www.intel.com/content/www/us/en/my-intel/sign-in-help.html>. Accessed: 2018-04-20.
- ISACA (2018). State of cybersecurity 2018 (part 1: Workforce development). [https://cybersecurity.isaca.org/state-of-cybersecurity?cid=pr\\_1230145&appeal=pr](https://cybersecurity.isaca.org/state-of-cybersecurity?cid=pr_1230145&appeal=pr). Accessed: 2018-04-23.
- Northcutt, S. (2018). Security controls. <https://www.sans.edu/cyber-research/security-laboratory/article/security-controls>. Accessed: 2018-04-20.
- Security, M. (2018). Security budgets increasing, but qualified cybertalent remains hard to find. <https://www.securitymagazine.com/articles/88940-security-budgets-increasing-but-qualified-cybertalent-remains-hard-to-find>. Accessed: 2018-04-23.



# A Screen shot of the Supplier Email

Intel Supplier e-Commerce Support Phone Menu and Service Request Form Changes Inbox x

 **Supplier Presence Site Notification** <supplier.presence.site.notification@intel.com>  
to 



April 24, 2018

## Intel Supplier e-Commerce Support Phone Menu and Service Request Form Changes

Suppliers will now have a simpler and more effective way to get help.

**Who is Affected:**

Suppliers with Websuite (PO/Invoice/Payment Tracker/Forecast/SIMI TSM) access.

**When:**

Starting 24 April 2018.

**Benefits/Impact:**

Phone Menu

The phone menu was recently redesigned to reflect a simplified set of options to getting support. This change removes the multi-tier menu, enabling quick access to the new phone menu options are listed as below:

As Is Phone Menu Option		To-Be Phone menu Option	
1	Inquiries about Purchase Order and Accounts Payable	1	Purchasing, Invoicing or Payment and Supplier Issues.
2	Problem with <a href="http://supplier.intel.com">supplier.intel.com</a> portal	2	"Empty/blank"

Service Request Form

For Service Request Form submission, a ticket number will be automatically assigned upon submission of request.

**Service Request Form**

**Thank you for submitting your request!**

A confirmation email has been sent to **request123@test.com** with the following ticket number for your tracking.

**INCO07112858**

Please use the above ticket number when interacting with Intel Support team.

**Notes:**  
Please refer to [Self Help Articles](#) for faster resolution to your support needs.  
Select the most relevant category for self-service.