



**GOVERNOR ERIC J. HOLCOMB'S  
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY**  
302 West Washington Street, IGC-South, Room E208  
Indianapolis, IN 46204

Welcome to the State of Indiana's Cybersecurity Scorecard in partnership with Purdue University!

This Scorecard should take you approximately 10-15 minutes to complete.

For your convenience, this Scorecard is a fillable PDF, can be saved with your answers, and will automatically calculate your score.

For your reference there is a Glossary of Terms on the last page with definitions for technical terms highlighted in blue lettering.

If you have any questions on this Scorecard, please email the Cybersecurity Program Director Chetrice Mosley at [mosleyclm@iot.in.gov](mailto:mosleyclm@iot.in.gov).

Name of Organization

---

Your E-mail Address

---

How many employees are there in your organization (full and part time)?

---

How many employees have information technology related duties?

---

How many employees have cybersecurity related duties?

---

Does your organization outsource your information technology needs?

Yes

No

Does your organization outsource your cybersecurity needs?

Yes

No

Question 1

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our organization values cybersecurity.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 2

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We know the type of data our organization stores (financial, health, customer, proprietary, trade secrets, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 3

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have evaluated the operational need of my data and systems to our organization's function (If we are a grocery store, we need to set pricing, scan barcodes, weigh produce, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 4

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our business/organization model influences the way we approach cybersecurity.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 5

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
When we make a decision in our organization that involves legal, operational, technological, or physical/environmental (office space) change, we consider cybersecurity as part of that decision.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 6

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We are familiar with the cybersecurity threats or risks (malicious software, phishing, and/or data breaches) to our organization specifically to our operations, reputation, inventory, customers, and employees.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 7

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We apply physical (doors and locks) controls in the same way we apply computer (ID and password) controls.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 8

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have <b>system checks</b> in place to make sure that our data is not compromised or changed.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 9

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our data is available to employees or clients when needed. (If our government or commerce site was unavailable to customers or employees, we would know what to do).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 10

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
As with the general policies in our organization, (dress code, paid time off, benefits, tardiness) we have policies that apply to cybersecurity.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 11

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
Our cybersecurity technology (such as <b>antivirus</b> , wireless access points, network equipment, etc.) is updated/configured to best protect our business operations and data.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 12

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have a process in place to address a <b>cyberthreat</b> .	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 13

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
We have a cyber emergency response plan in place to address a <b>cyberattack</b> on our organization.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 14

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
If we were impacted by a cyber emergency (e.g. <b>ransomware</b> ), we know how our organization would recover our data and/or operational systems.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 15

	I Don't Know (0)	Strongly Disagree (1)	Disagree (2)	Neither Agree or Disagree (3)	Agree (4)	Strongly Agree (5)
After a <b>cyberthreat</b> or emergency, our organization will make changes to people, process, technology, etc. to improve our security.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 16

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
Our executive leadership receives periodic status, physical, and cybersecurity updates.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 17

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We keep an inventory of our data (customer, payroll, and/or financial data) and devices that provide access to our data.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 18

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We provide our employees cybersecurity awareness and/or training.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 19

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We protect our business and customer information so that only the employees that need to see it, can.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 20

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
We would know if our cybersecurity technology detected a <b>cyberthreat</b> .	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 21

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are not connected to a publicly available internet connection.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Question 22

	I Don't Know (0)	Never (1)	Almost Never (2)	Occasionally /Sometimes (3)	Almost Every Time (4)	Every Time (5)
Our 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) are periodically monitored and scanned for security vulnerabilities and malicious software	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

To find your score, please add the numbers associated with the responses for questions 1 through 22. For example, selecting “Almost Every Time (4)” has a numerical value of 4.

Your score is \_\_\_\_\_

Refer to the chart below to determine where you fall on the scale.

Grade	Exemplary	Accomplished	Developing	Beginning	Undeveloped
Minimum with color code	88	66	44	22	0
Range	110-88	87-66	65-44	43-22	21-0
Spread	22	21	21	21	21

## Glossary of Terms

**System checks**- procedures, equipment, and/or periodic inspection to maintain security

**Antivirus**- i.e. McAfee, Norton, or Windows Defender

**Cyberthreat**- the possibility of a malicious attempt to damage or disrupt a computer network or system. For example, social engineered trojans, unpatched software (such as Java, Adobe Reader, Flash), and/or phishing

**Cyberattack**- an attack initiated from one or more computers against a website, computer system or a networked enterprise of several computers that compromises the confidentiality, integrity or availability of any computer(s) or stored information

**Ransomware**- a type of malware that prevents users from using their computer and displays messages requiring users to pay a ransom usually through an online payment in order to regain access to his/her computer, information, and/or system.