NORTH RISK PARTNERS®

CYBER INSURANCE & RISK MANAGEMENT

OCTOBER 2023

PRESENTERS

JEANINE LOOMIS
Senior Vice President
RT Specialty

AMOS AESOPH
Chief Information Security Officer
Xigent

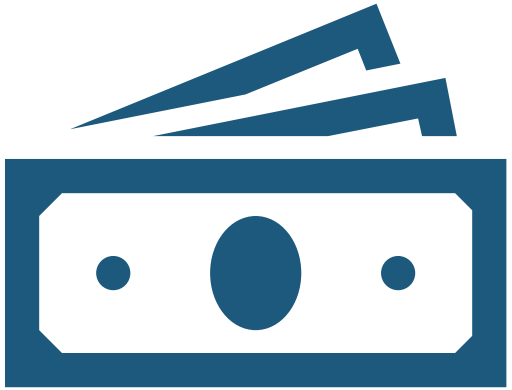
NEIL FINK
Risk Advisor
North Risk Partners

ANDREW SCHMELZLE
Senior Account Executive
Xigent

NORTH RISK PARTNERS®

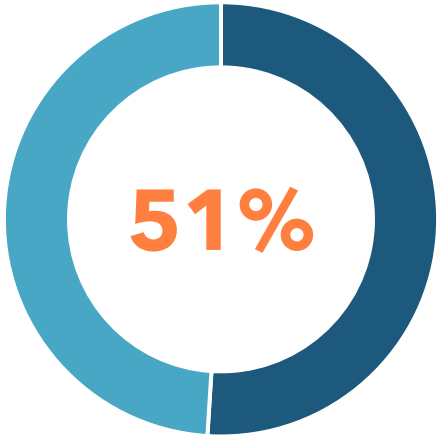
CYBER SECURITY LANDSCAPE

2023 IBM SECURITY REPORT

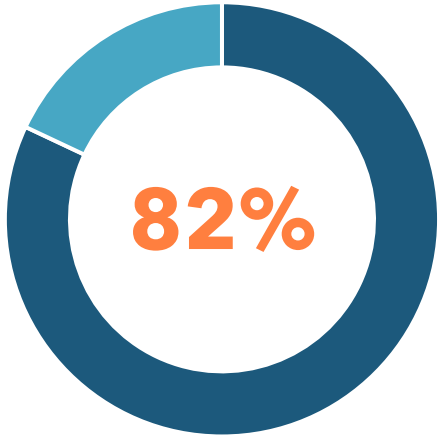


$4.5 million

The average cost of a data breach reached



51% of organizations plan to increase security investments as the result of a breach

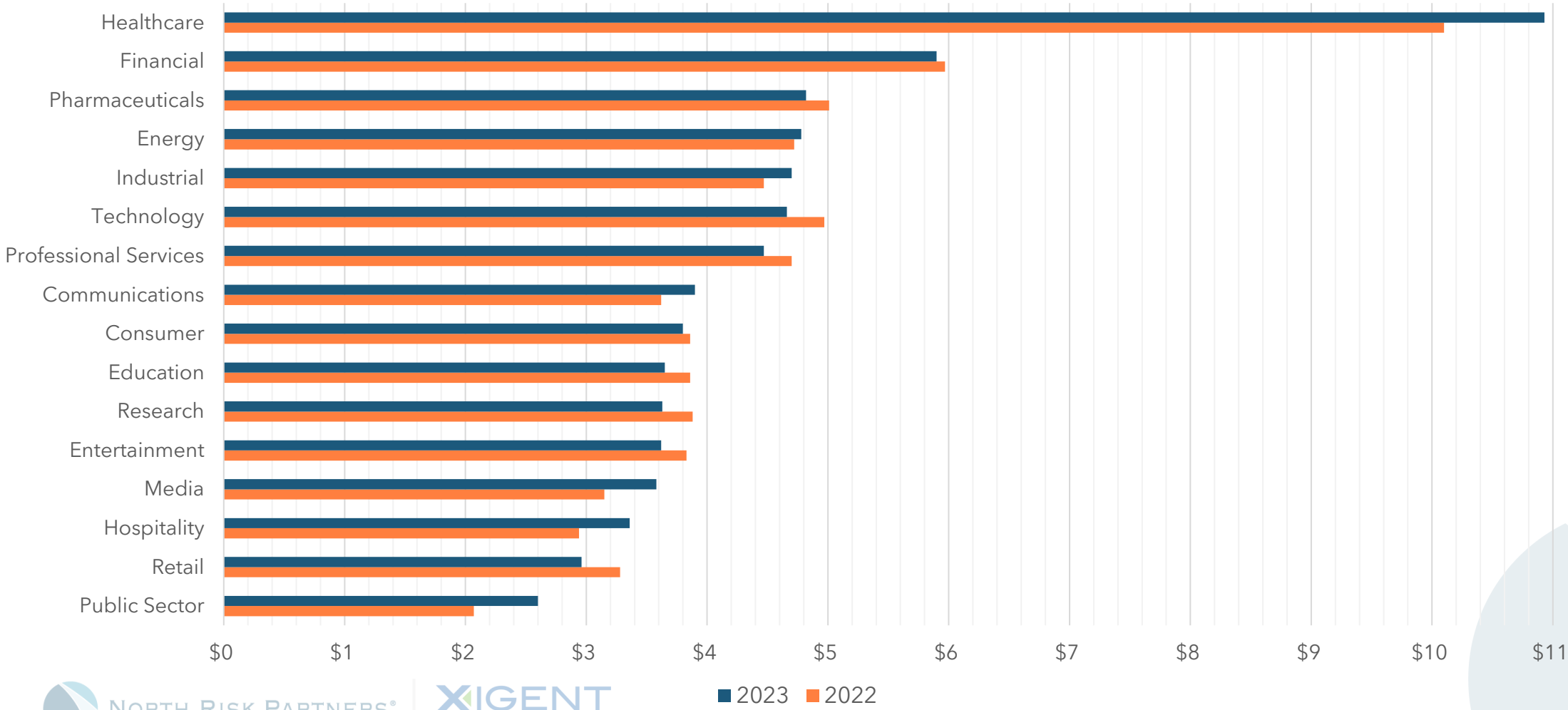


82% of breaches involved data stored in the cloud (public, private, or multiple environments)

NORTH RISK PARTNERS®

XIGENT
Result Driven IT

COST OF DATA BREACH BY INDUSTRY



NORTH RISK PARTNERS®

XIGENT
Result Driven IT

Source: 2023 Cost of a Data Breach Report by IBM Security and Ponemon Institute

THE RISING THREAT LANDSCAPE

RANSOMWARE

USB DRIVES

HACKTIVISM

MOBILE THREATS

ARTIFICIAL INTELLIGENCE

NORTH RISK PARTNERS®

CYBER INSURANCE MARKET

CHALLENGES OF THE CYBER INSURANCE MARKET

- MALWARE
- RANSOMWARE
- DISTRIBUTED DENIAL OF SERVICE (DDoS)
- ECONOMIC LOSSES
- UNDERWRITING & RATES

Source: What you need to know about the Cyber insurance market | SwissRe | August 28, 2023

NORTH RISK PARTNERS®

UNDERSTANDING CYBER INSURANCE COVERAGE

NO TWO POLICIES ARE THE SAME

3rd Party

- Network Security and Privacy Liability Limit
- Regulatory Liability Limit
- Media Liability Limit
- PCI DSS Liability Limit

NO TWO POLICIES ARE THE SAME

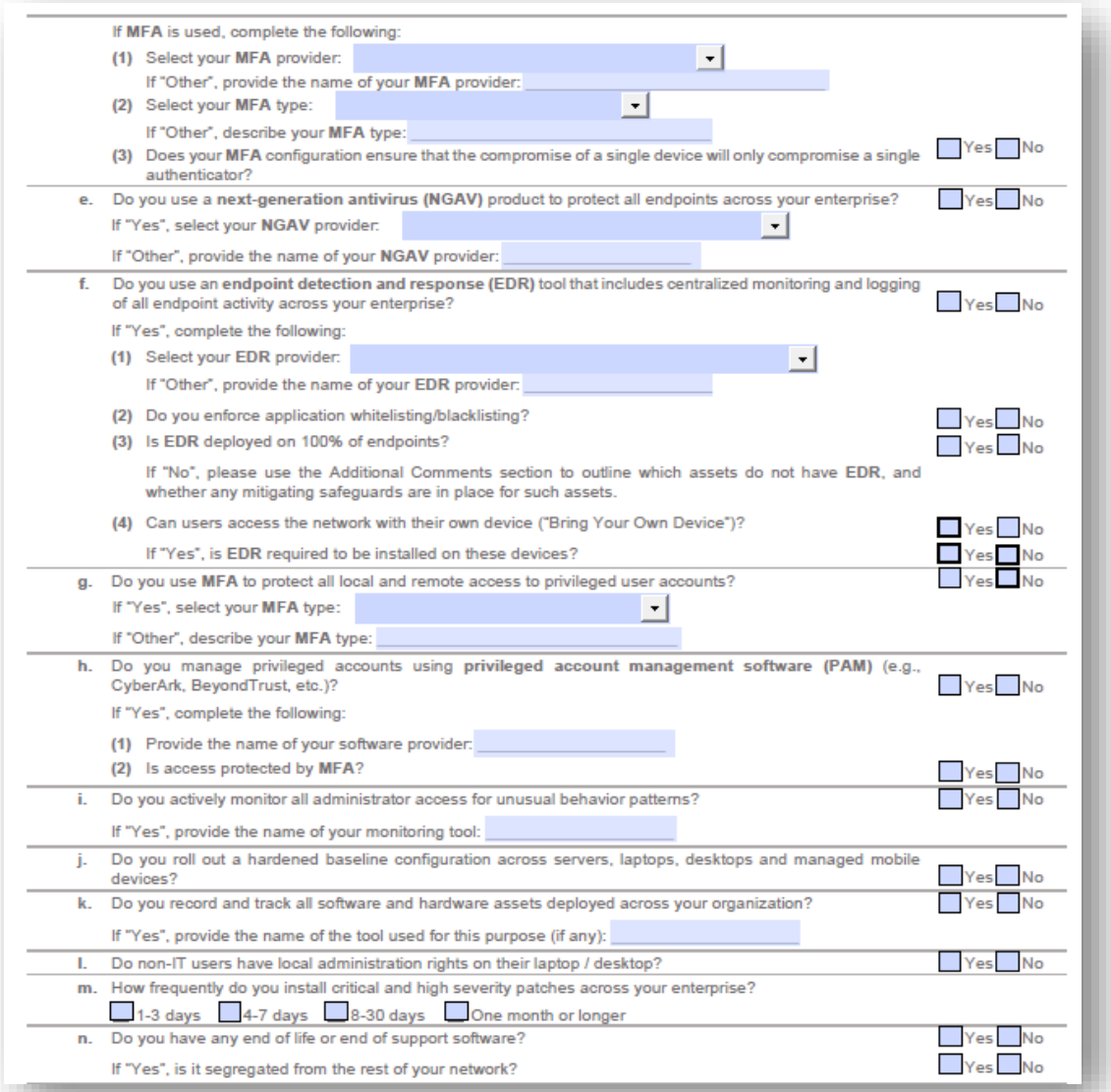
1st Party

- Cyber Extortion Limit
- Business Interruption Limit
- Contingent Interruption Limit
- System Failure Limit
- Contingent System Failure Limit
- Data Recovery Limit
- Reputational Harm Limit
- Social Engineering/Cyber Crime Limit
- Hardware Replacement Cost Limit

NORTH RISK PARTNERS®

THE APPLICATION & ASSESSING YOUR ORGANIZATION'S CYBER HYGIENE

USE THE APPLICATION AS A WORKING DOCUMENT



If **MFA** is used, complete the following:

(1) Select your **MFA** provider:

If "Other", provide the name of your **MFA** provider:

(2) Select your **MFA** type:

If "Other", describe your **MFA** type:

(3) Does your **MFA** configuration ensure that the compromise of a single device will only compromise a single authenticator? ☐ Yes ☐ No

e. Do you use a **next-generation antivirus (NGAV)** product to protect all endpoints across your enterprise? ☐ Yes ☐ No

If "Yes", select your **NGAV** provider:

If "Other", provide the name of your **NGAV** provider:

f. Do you use an **endpoint detection and response (EDR)** tool that includes centralized monitoring and logging of all endpoint activity across your enterprise? ☐ Yes ☐ No

If "Yes", complete the following:

(1) Select your **EDR** provider:

If "Other", provide the name of your **EDR** provider:

(2) Do you enforce application whitelisting/blacklisting? ☐ Yes ☐ No

(3) Is **EDR** deployed on 100% of endpoints? ☐ Yes ☐ No

If "No", please use the Additional Comments section to outline which assets do not have **EDR**, and whether any mitigating safeguards are in place for such assets.

(4) Can users access the network with their own device ("Bring Your Own Device")? ☐ Yes ☐ No

If "Yes", is **EDR** required to be installed on these devices? ☐ Yes ☐ No

g. Do you use **MFA** to protect all local and remote access to privileged user accounts? ☐ Yes ☐ No

If "Yes", select your **MFA** type:

If "Other", describe your **MFA** type:

h. Do you manage privileged accounts using **privileged account management software (PAM)** (e.g., CyberArk, BeyondTrust, etc.)? ☐ Yes ☐ No

If "Yes", complete the following:

(1) Provide the name of your software provider:

(2) Is access protected by **MFA**? ☐ Yes ☐ No

i. Do you actively monitor all administrator access for unusual behavior patterns? ☐ Yes ☐ No

If "Yes", provide the name of your monitoring tool:

j. Do you roll out a hardened baseline configuration across servers, laptops, desktops and managed mobile devices? ☐ Yes ☐ No

k. Do you record and track all software and hardware assets deployed across your organization? ☐ Yes ☐ No

If "Yes", provide the name of the tool used for this purpose (if any):

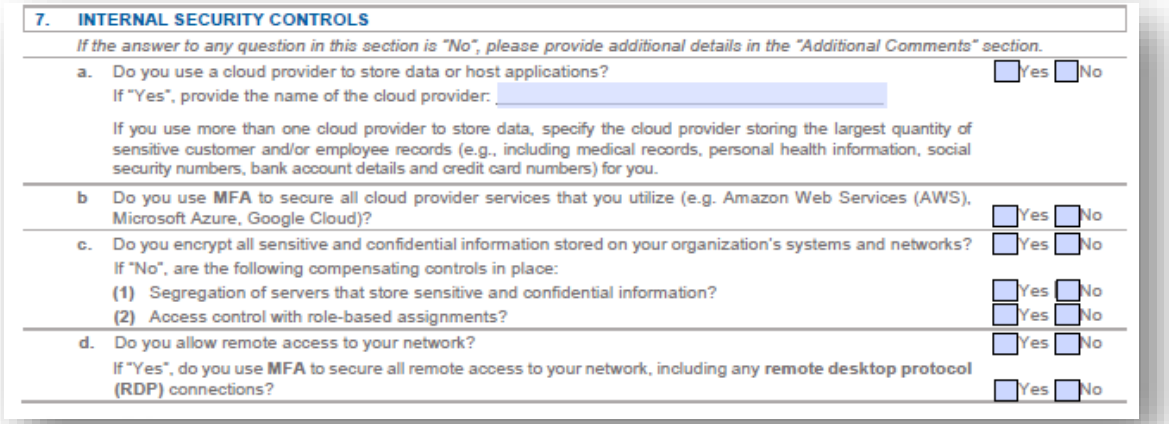
l. Do non-IT users have local administration rights on their laptop / desktop? ☐ Yes ☐ No

m. How frequently do you install critical and high severity patches across your enterprise?

☐ 1-3 days ☐ 4-7 days ☐ 8-30 days ☐ One month or longer

n. Do you have any end of life or end of support software? ☐ Yes ☐ No

If "Yes", is it segregated from the rest of your network? ☐ Yes ☐ No



7. INTERNAL SECURITY CONTROLS

If the answer to any question in this section is "No", please provide additional details in the "Additional Comments" section.

a. Do you use a cloud provider to store data or host applications? ☐ Yes ☐ No

If "Yes", provide the name of the cloud provider:

If you use more than one cloud provider to store data, specify the cloud provider storing the largest quantity of sensitive customer and/or employee records (e.g., including medical records, personal health information, social security numbers, bank account details and credit card numbers) for you.

b Do you use **MFA** to secure all cloud provider services that you utilize (e.g. Amazon Web Services (AWS), Microsoft Azure, Google Cloud)? ☐ Yes ☐ No

c. Do you encrypt all sensitive and confidential information stored on your organization's systems and networks? ☐ Yes ☐ No

If "No", are the following compensating controls in place:

(1) Segregation of servers that store sensitive and confidential information? ☐ Yes ☐ No

(2) Access control with role-based assignments? ☐ Yes ☐ No

d. Do you allow remote access to your network? ☐ Yes ☐ No

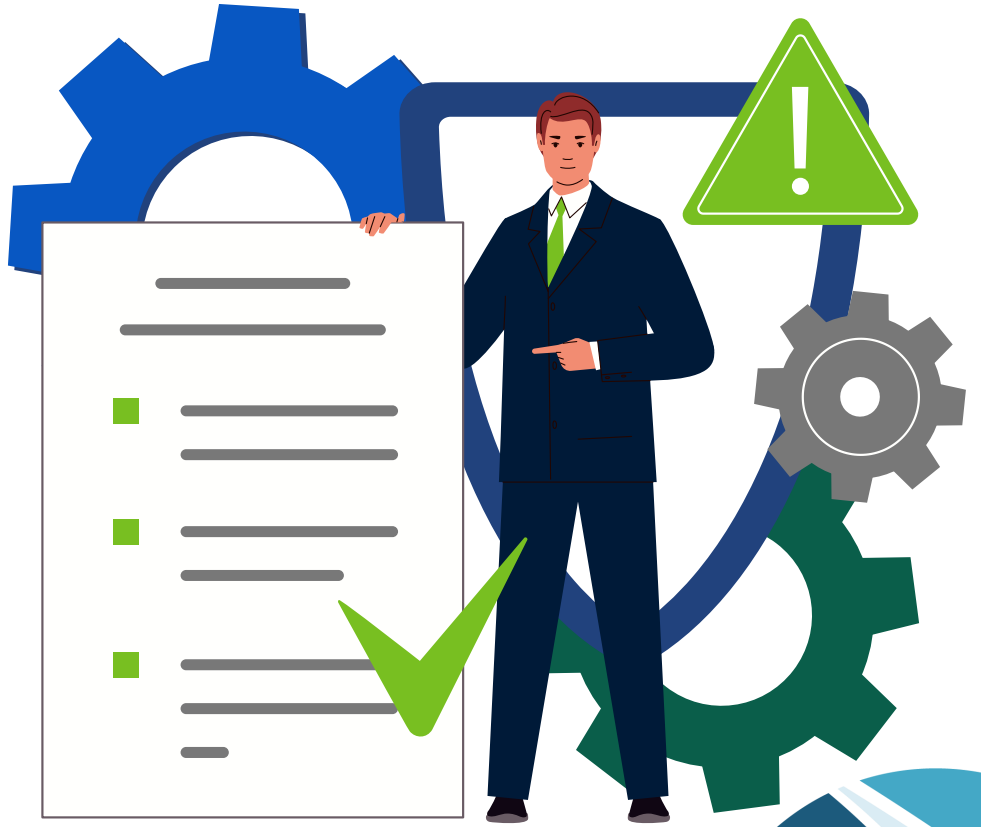
If "Yes", do you use **MFA** to secure all remote access to your network, including any **remote desktop protocol (RDP)** connections? ☐ Yes ☐ No

- Work with the head of IT to complete the application
- Always add an addendum to better explain your company
- Ask questions of your IT provider to understand the controls you do or don't have in place
- Remember that you are never fully secure. Keep working on your Controls & Cyber Hygiene

STRATEGIES FOR CYBER LIABILITY PROTECTION

Proactive Measures to Protect from Cyber Liability

- Employee training and awareness programs
- Understanding where your data lives (hardware, software, cloud)
- Regular software updates and patch management
- Strong authentication methods (multi-factor authentication)
- Cybersecurity insurance coverage
- Utilize available cybersecurity frameworks



North Risk Partners®

XIGENT Result Driven IT

NORTH RISK PARTNERS®

PRACTICAL TIPS

THE HUMAN FACTOR

- Use the Risk Management Services offered by your cyber insurance carrier
- Continually educate your employees about the risks
- Have employees verify any new funds transfer request by phone (and don't use the phone # on the email or respond to the email)
- If you haven't created an Incident Response Plan – create one, run through it and PRINT IT OUT. If you already have one, when was the last time you reviewed it with your team? Have you performed a tabletop exercise?
- If you purchase a cyber insurance policy, make sure ALL of the members of your Incident Response Team have access to the Hotline Phone #
- Audit your data. Do you still need to hold on to the information you are storing?

QUESTIONS?