WHEN FAILURE IS NOT AN OPTION:

FORTUNE 500 COMPANIES WEIGH IN ON EQUIPMENT FAILURE

FM Global®

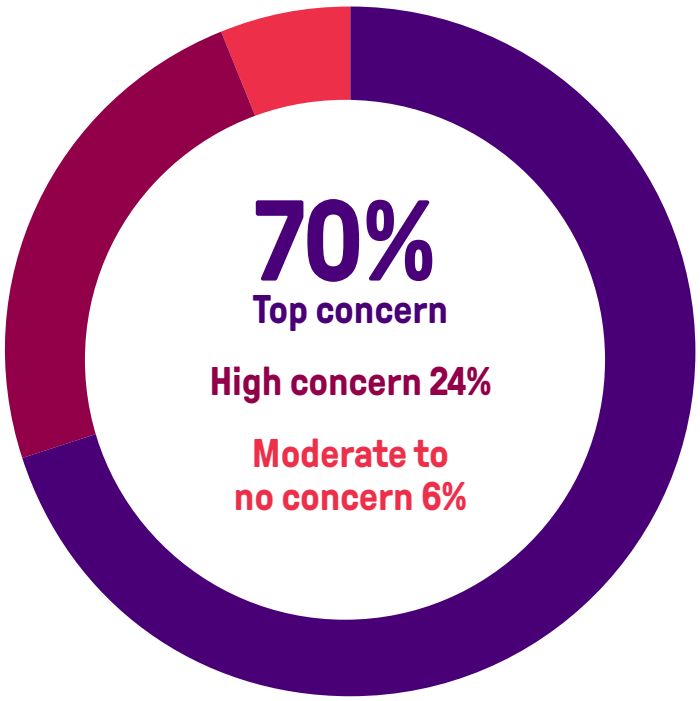
Failure of critical equipment can severely disrupt a business. The risk of such failure is rising, and internet connections are raising the specter of cyber attack on industrial controls. These findings and more are documented in the following results of FM Global's survey of 200 business leaders at Fortune 500-size companies. All respondents have companywide responsibility for overseeing equipment operations or equipment risk.

1

Equipment failure is a major concern for Fortune 500-size companies.

To what extent are the risks associated with the failure of critical equipment (e.g., explosion, fire, cyber breach, breakdown) a concern for you?

LEVEL OF CONCERN:



2

The risk of equipment failure is rising.

EQUIPMENT FAILURE RISKS OVER THE PAST 5 YEARS:

MAIN REASONS:

- More equipment in use (53% of respondents)
- High demand due to healthy economy (45%)
- Aging equipment (42%)
- Increased operator turnover (40%)
- High cost of suspending production lines (40%)
- Lack of maintenance (39%)
- Lack of experienced operators (39%)
- Lack of training (37%)
- Aging workforce (34%)
- Repairs too costly (33%)

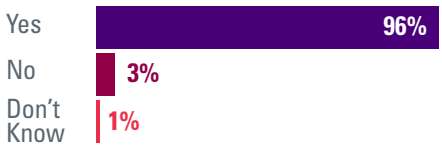
Have the risks associated with the failure of critical equipment increased, decreased or remained the same in your organization over the past 5 years?

If so, why do you say that?

3

Most companies' industrial control systems (ICS) are connected to the internet and could be vulnerable to hacking.

ICS CONNECTED TO THE INTERNET:



Do your industrial control systems connect to the internet?

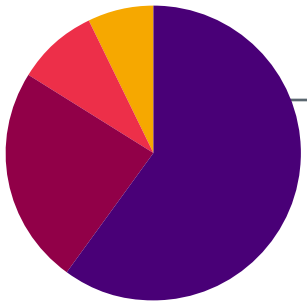
CONCERNED ABOUT HACKING:

Top Concern 60%

High Concern 24%

Moderate Concern 9%

Low Concern 7%



84% Major Concern

How concerned are you that a hacker could breach your industrial control systems?

4

The business consequences of equipment failure could be significant.

Decline in Revenue/Earnings
54% of respondents

Increased Scrutiny from Investors
51%

Introduction of Regulatory Compliance Problems
50%

Degradation of Brand/Reputation
48%

Inability to Fulfill Orders
46%

Decline in Share Price
39%

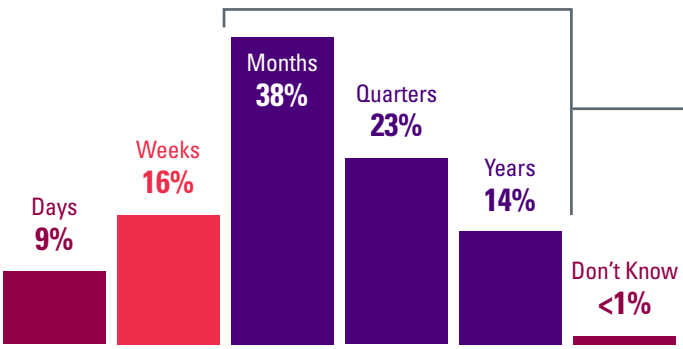
Layoffs/Loss of Key Employees
29%

If your organization had a failure of critical equipment, what would you expect to be the impact?

5

Financial recovery time could be lengthy for companies.

FINANCIAL RECOVERY TIME:



75% of companies report that it could take at least ***months*** to recover financially from the failure of critical equipment.

How quickly would you expect your organization to financially recover from the failure of critical equipment?

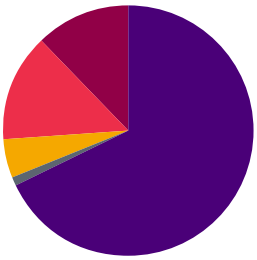
In Conclusion

As this report shows, the risk of equipment failure weighs heavily on the minds of Fortune 500 business leaders, and it should. A robust economy, turnover in the technical workforce and an increasingly potent cyber criminal community means every company should be scrutinizing its potential vulnerabilities now. If companies don't take measures to prevent equipment failure, they put their business resilience at risk.

Methodology and Respondent Profile

Research was commissioned by FM Global and conducted in September 2019 by Engine, a global market research firm.

BUSINESS LEADERS WITH CORPORATE OVERSIGHT OF EQUIPMENT



COMPANY SIZE (US$)

$1-4.9BN 26%

$5-9.9BN 23%

$10-19.9BN 26%

$20BN+ 25%

What were your organization's worldwide revenues, in U.S. dollars, in its most recent fiscal year?

What role do you play in managing risks associated with critical equipment failure?