ADVISORY BOARD for the ARTS

Transforming Arts Organizations Worldwide

Arts Organization Leader Benchmarking

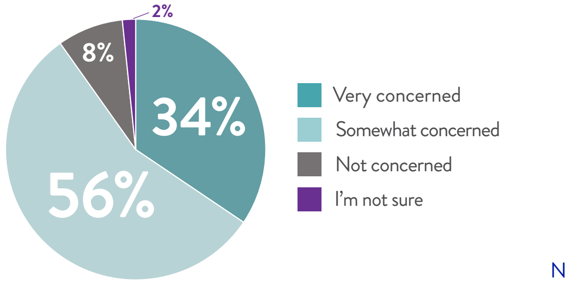
MARCH 21, 2023

The Advisory Board for the Arts regularly surveys leaders at arts organizations — including operas, ballets, symphonies, festivals, theaters, venues, schools, advocacy organizations, and museums — about issues relevant to the arts world. This online survey was fielded **March 6–15, 2023**. This is the sixty-ninth survey of the series and was designed to help arts leaders benchmark themselves on organizations' overall preparedness and concern around cyber security breaches, the state of their disaster protocols and training, as well as any advice for working with external contractors/advisors.

BUDGET & STATE OF CYBERSECURITY

Overwhelming Majority Are Concerned About Future Cyberattacks

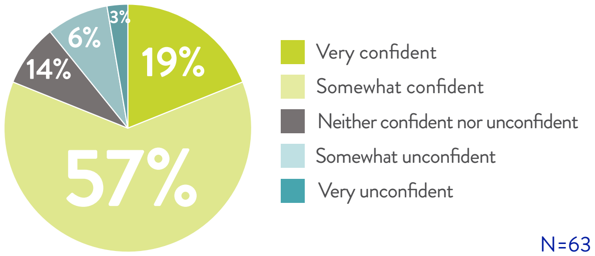
Level of Concern About Potential Cyber/Ransom Attack at Org



N=61

Orgs Generally Feel Prepared for Potential Cyberattacks

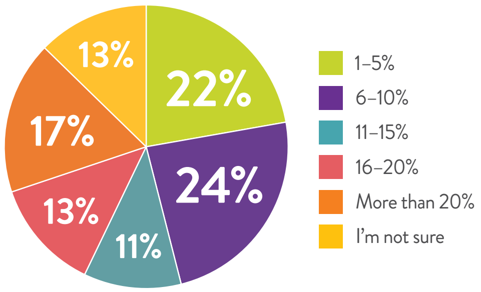
Confidence in Overall Org Security to Prevent, Detect, and Respond to a Cyberattack



N=63

Range of Budgets Allocated Towards Cybersecurity

% of Current Overall IT Budget Allocated to Cybersecurity



N=63

Cybersecurity Budgets Have Increased From Last FY's Budget

+24.7%

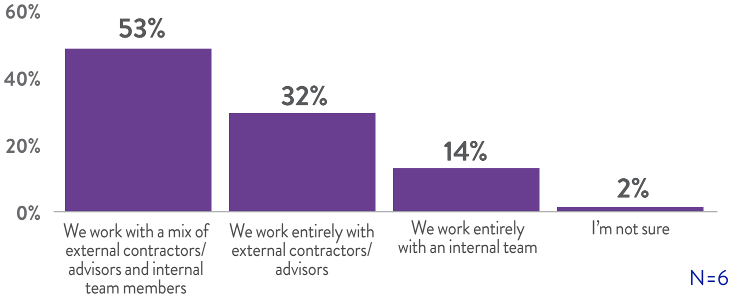
Average percentage change in organization's current overall IT budget towards cybersecurity measures compared to that of the most recent fiscal year.

N=36

CYBERSECURITY STAFFING

Half Work with a Mix of External Contractors and Internal Team Members

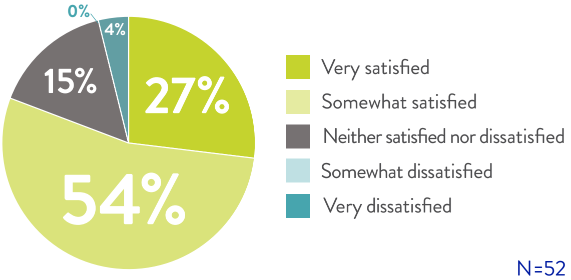
Staffing Structure of Cybersecurity Needs



N=63

Majority Are Happy with External Cybersecurity Support

Satisfaction with Current External Cybersecurity Contractors



N=52

ADVISORY BOARD for the ARTS

Transforming Arts Organizations Worldwide

Arts Organization Leader Benchmarking

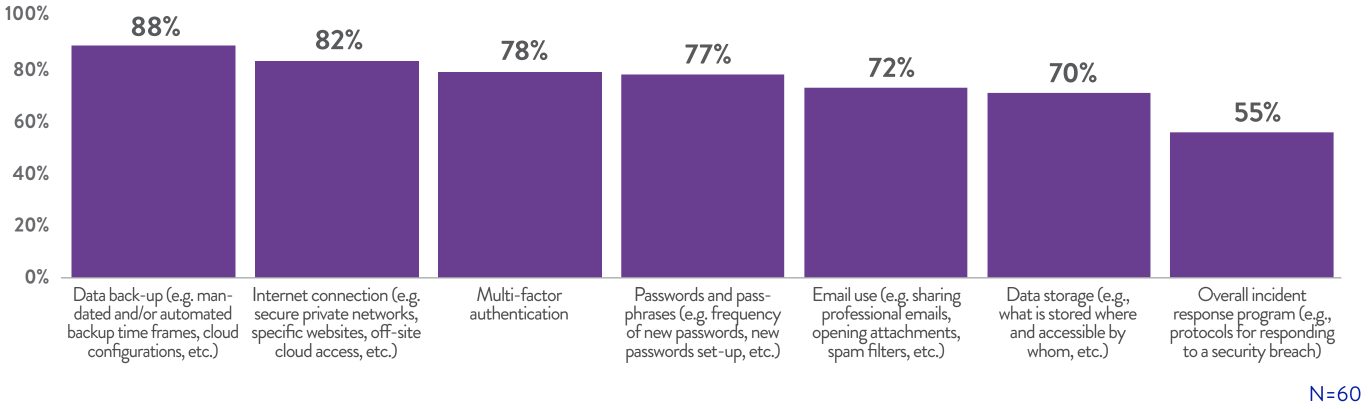
MARCH 21, 2023

The Advisory Board for the Arts regularly surveys leaders at arts organizations — including operas, ballets, symphonies, festivals, theaters, venues, schools, advocacy organizations, and museums — about issues relevant to the arts world. This online survey was fielded **March 6–15, 2023**. This is the sixty-ninth survey of the series and was designed to help arts leaders benchmark themselves on organizations' overall preparedness and concern around cyber security breaches, the state of their disaster protocols and training, as well as any advice for working with external contractors/advisors.

CURRENT CYBERSECURITY POLICIES

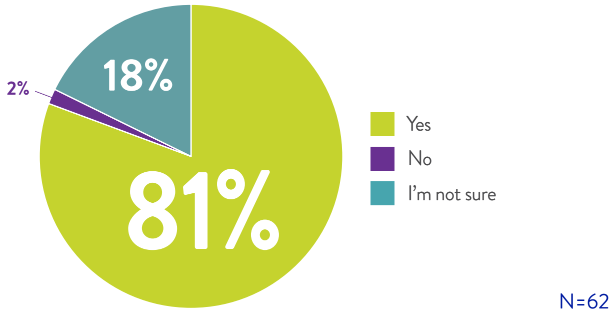
Fewer Orgs Have Formal Policies for Incident Responses Compared to Other Areas

Formal Cybersecurity Policies/Protocols in Place



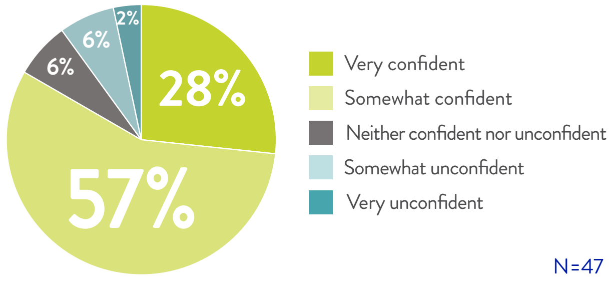
Most Orgs Have Payment Gateway Systems

Existence of Payment Gateway Systems to Protect Online Payments



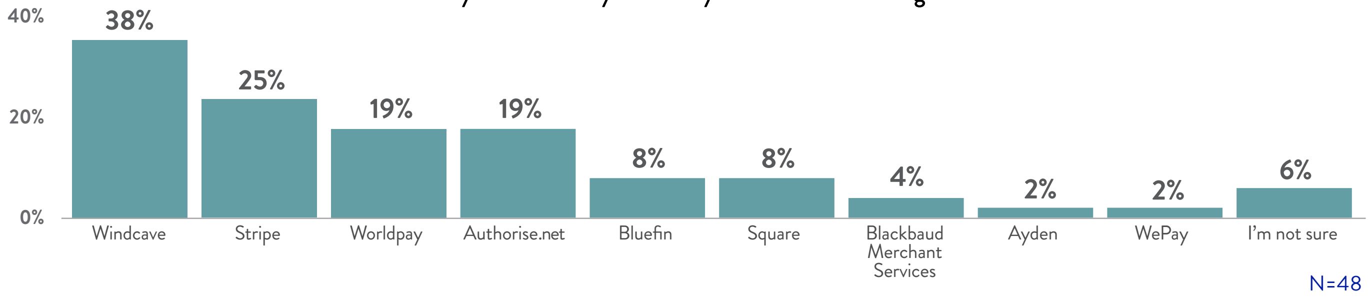
Over 80% Are Confident with Their Payment Gateway Systems

Confidence with Security Services Provided by Payment Gateway Systems



Wide Selection of Payment Gateways in Use

Payment Gateways in Use by Arts and Culture Orgs



ADVISORY BOARD for the ARTS
Transforming Arts Organizations Worldwide

Arts Organization Leader Benchmarking

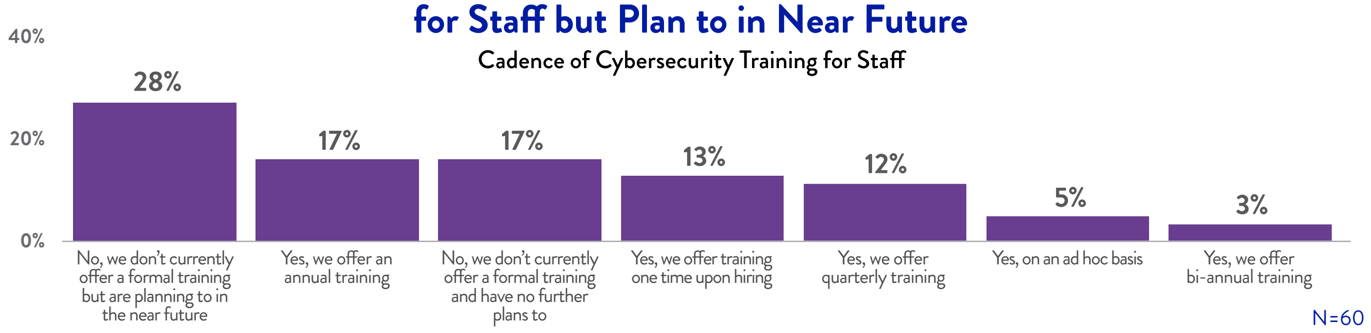
MARCH 21, 2023

The Advisory Board for the Arts regularly surveys leaders at arts organizations — including operas, ballets, symphonies, festivals, theaters, venues, schools, advocacy organizations, and museums — about issues relevant to the arts world. This online survey was fielded **March 6–15, 2023**. This is the sixty-ninth survey of the series and was designed to help arts leaders benchmark themselves on organizations' overall preparedness and concern around cyber security breaches, the state of their disaster protocols and training, as well as any advice for working with external contractors/advisors.

TRAINING & DISASTER PROTOCOLS

One-Quarter Do Not Currently Offer Formal Cybersecurity Training for Staff but Plan to in Near Future

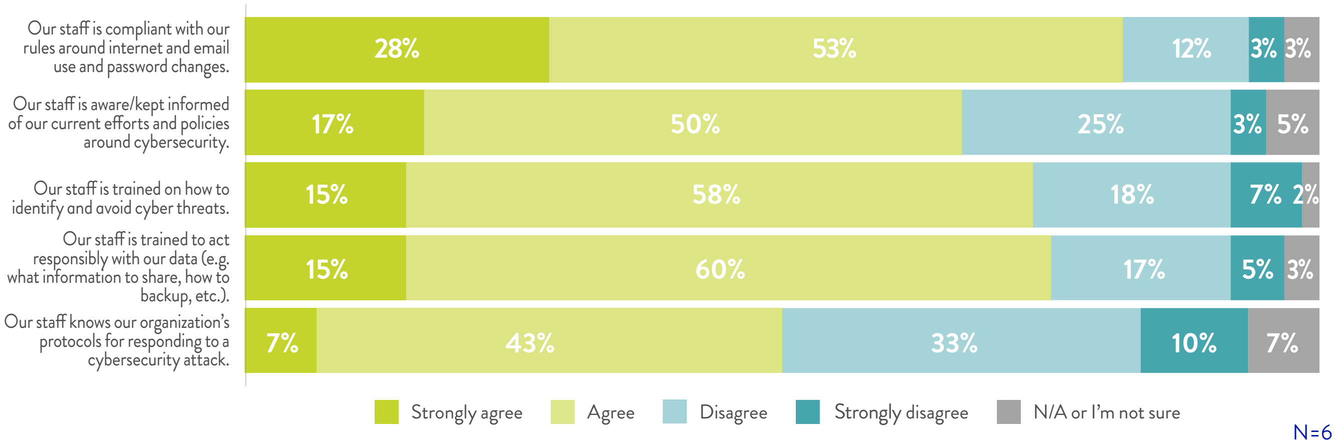
Cadence of Cybersecurity Training for Staff



N=60

Potential for Orgs to Increase Staff Knowledge of Org Protocols for Responding to a Cybersecurity Attack

Agreement Level to Statements Around Staff's Training/Preparedness for Cyberattacks



N=60

Advice/Lessons Learned for Orgs Looking to Improve Their Cybersecurity Measures

Getting outside input from consultants is a must and getting deeper knowledge and experience from multiple clients. Use Multifactor Authentication!

Perform an annual third party penetration test; run sophisticated endpoint protection and hire a third party SOC; test and train staff monthly; and build an incident response and business continuity plan.

Be proactive, not reactive.

You can never train your staff enough. Do not wait until it is too late.

Be open on where you are currently lacking when hiring on someone who knows their stuff about cyber security. Oftentimes, those in IT are willing to share their own knowledge, background, and programs to assist.

Regular communication with staff about what to look out for is key and always provide examples. And give staff a dedicated channel to report suspicious emails/calls.